IMAGINEX GROUP

STAFF HANDBOOK | HONG KONG

Contents

MESSAGE FROM THE PRESIDENT 5
FOREWORD 6
ABOUT IMAGINEX GROUP 7
HISTORY 9
VISION20:20 11
HUMAN RESOURCES PRACTICE 12
DEFINITIONS, INTERPRETATION AND GUIDANCE 13

PART A: POLICIES SPECIFIC TO IMAGINEX GROUP

1. EMPLOYMENT 15
   - 1.1 Hiring
   - 1.2 Probation
   - 1.3 Transfer and Secondment
   - 1.4 Termination of Employment
   - 1.5 Retirement
   - 1.6 Certification of Employment

2. WORKING HOURS 17
   - 2.1 Overtime/Time Off

3. COMPENSATION AND BENEFITS 17
   - 3.1 Salary
   - 3.2 Annual Bonus
   - 3.3 Annual Salary Review
   - 3.4 Sales Commission/Incentives
   - 3.5 Employee Compensation
   - 3.6 Medical & Dental Schemes
   - 3.7 Pension
   - 3.8 Business Travel Insurance
   - 3.9 Employee Purchase Privilege

4. HOLIDAYS AND LEAVE 21
   - 4.1 Annual Leave
   - 4.2 Statutory/Public Holidays
   - 4.3 Rest Days
   - 4.4 Birthday Leave
   - 4.5 Anniversary Leave
   - 4.6 Sick Leave
   - 4.7 Compensation Leave
   - 4.8 Marriage Leave
   - 4.9 Maternity Leave
   - 4.10 Paternity Leave
   - 4.11 Adoption Leave
   - 4.12 Compassionate Leave
   - 4.13 Examination Leave
   - 4.14 Jury Service Leave
   - 4.15 Unpaid Leave
   - 4.16 Leave Application

5. PEOPLE DEVELOPMENT 29
5.1 Performance Management System
5.2 Learning & Development
5.3 Continuous Training

6. RULES & REGULATIONS 30
6.1 Attendance
6.2 Business Cards
6.3 Telephones
6.4 Mail

7. HANDLING OF COMPANY ASSETS 31
7.1 Company Files and Accounts
7.2 Use of Office Equipment and Other Company's Resources
7.3 Refreshment
7.4 Name Badge
7.5 Lost Property

8. COMMUNICATIONS/EMPLOYEE RELATIONS 32
8.1 Staff Recreation Committee
8.2 Press Articles
8.3 Photography Policy at One Island South
8.4 Disciplinary Action and Suspension

PART B: GENERAL POLICIES ACROSS ALL LANE CRAWFORD JOYCE GROUP COMPANIES

INTRODUCTION 34

GROUP POLICIES 36

1. MAINTAINING A HEALTHY AND SAFE WORKPLACE 36
1.1 Co-operation between Employees and Company
1.2 Hygiene, Fire Precautions and First Aid
1.3 Workplace Security
1.4 Stock Security
1.5 Smoking, Alcohol and Drugs
1.6 Reporting an Accident or Injury
1.7 Employee Wellbeing
1.8 Typhoons, Rainstorms and Other Adverse Weather

2. PROFESSIONALISM, FAIRNESS AND RESPECT FOR OTHERS 42
2.1 Employee Code of Conduct
2.2 Equal Employment Opportunities
2.3 Protection against Discrimination, Harassment, Vilification and Victimisation
2.4 Disclosure of Criminal Convictions

3. FORMAL GRIEVANCE PROCEDURE 45
3.1 Principles
3.2 Grievance Procedure
3.3 Anonymous Grievance Claims

4. POLITICAL NEUTRALITY 49
4.1 Expressing Political Views in the Workplace
4.2 Time Away from the Workplace for Political Activities

5. PROTECTION OF COMPANY'S CONFIDENTIAL INFORMATION 49
5.1 What is Confidential Information?
5.2 Employee Obligations in relation to Confidential Information
5.3 Duration of Confidentiality Obligations and Consequences of Breach

6. PROTECTION OF INTELLECTUAL PROPERTY RIGHTS 51
6.1 What are Intellectual Property Rights?
6.2 Protection of Intellectual Property Rights belonging to the Company or Third Parties
6.3 Intellectual Property Rights in Company Innovations
6.4 Survivability of Rights and Obligations relating to Intellectual Property

7. PROTECTION OF PERSONAL DATA PRIVACY 52
7.1 Overview of Personal Data Obligations in Hong Kong
7.2 Company's Collection and Use of Employees' Personal Data
7.3 Company's Collection and Use of Customers' Personal Data
7.4 Company's Collection and Use of Third Parties' Personal Data
7.5 Violations of this Policy
7.6 Further Information

8. ANTI-CORRUPTION 63
8.1 Zero Tolerance of Corruption
8.2 Bribery
8.3 Corrupt Acts of Third Parties
8.4 Other Potential Red Flags
8.5 Who to Contact to Raise Concerns or Seek Guidance about Corruption

9. INTERNAL FINANCIAL WRONGDOING 67
9.1 Please Speak Up
9.2 Fraud
9.3 Business-related Expenses
9.4 Business-related Gifts and Hospitality
9.5 Charitable Contributions
9.6 Political Contributions
9.7 Who to Contact to Raise Concerns or Seek Guidance about Internal Financial Wrongdoing
9.8 Responsibility for Internal Financial Wrongdoing Policy

10. CONFLICTS OF INTEREST AND OUTSIDE WORK 73
10.1 Employee Conflicts of Interest
10.2 Employee Declaration of Conflicts of Interest
10.3 Some Examples of Conflicts of Interest
10.4 Failure to Declare Conflicts of Interest
10.5 Conflicts of Interest and Outside Work
10.6 Private Transactions

11. FAIR BUSINESS PRACTICES & COMPLIANCE WITH COMPETITION LAW 76
- 11.1 Scope of Competition Law Obligations
- 11.2 Anti-Competitive Agreements
- 11.3 Exchanging Information with Competitors
- 11.4 Abuse of Power in the Market
- 11.5 Training and External Communications
- 11.6 How to Raise Concerns or Seek Guidance about Competition Law

12. WHISTLEBLOWING 79
- 12.1 Definitions used in this Whistleblowing Policy
- 12.2 Protection of Whistleblowers
- 12.3 Confidentiality
- 12.4 Making a Whistleblowing Report
- 12.5 Investigation Procedures for Whistleblower Complaints
- 12.6 Retention of Records of Whistleblowing

13. COMMUNICATIONS WITH THE MEDIA 82
- 13.1 No Media Communication Without Authorisation
- 13.2 Handling Direct Requests from Media
- 13.3 Media Training

14. USE OF SOCIAL MEDIA AND OTHER PUBLIC COMMUNICATION PLATFORMS 82
- 14.1 Scope of Policy
- 14.2 No Social Media Communications on behalf of the Company without Authorisation
- 14.3 Acting Responsibly
- 14.4 Confidential Information and Social Media
- 14.5 Guidance on Social Media Best Practices

15. CCTV AND IN-STORE PHOTOGRAPHY POLICY 85
- 15.1 In-Store Photography
- 15.2 Closed Circuit Television (CCTV) Recording

16. USE OF COMPANY'S ELECTRONIC SYSTEMS & CONTENT 89
- 16.1 What are the Company's Electronic Systems?
- 16.2 Use of the Company's Electronic Systems
- 16.3 Ownership of Electronic Content
- 16.4 Security of the Company's Electronic Systems and Content
- 16.5 Preservation, Monitoring and Review of the Company's Electronic Systems and Content
- 16.6 No Expectation of Privacy
- 16.7 Network Management
- 16.8 Bring Your Own Device (BYOD) policy
- 16.9 Notice of Data Protection Compliance

17. DAWN RAIDS (SEARCHES OF COMPANY PREMISES & DEMANDS FOR COMPANY INFORMATION OR PROPERTY) AND BUSINESS SCAMS 96
- 17.1 What is a Dawn Raid?
- 17.2 What to do in a Dawn Raid
- 17.3 Business Scams and Other Fraudulent Demands

18. THIRD PARTY RIGHTS UNDER EMPLOYMENT CONTRACTS 99

ACCEPTANCE OF THE HANDBOOK 100

MESSAGE FROM THE PRESIDENT

Welcome to Imaginex!

We believe in our people.

Your energy, passion and creativity drive us forward.

I am very happy that you have become a part of our big family.

Many thanks to our dedicated team, we have expanded from just one store in Hong Kong in 1993 to more than 500 stores today in Mainland China, HK, Taiwan, Macau and Singapore, with over 2,500 frontline and supporting staff across 54 cities in Mainland China and South East Asia.

Imaginex has developed a caring company culture to nurture our employees. We provide professional training programmes and career development opportunities, both locally and regionally. We also strive to foster a happy and conducive workplace where you can contribute your talent to our success story.

To start the journey with us, please take the time to read this Staff Handbook thoroughly where you can find more information about the Imaginex Group, our policies and guidelines, and your benefits and obligations. When in doubt, talk to your Line Manager, your Human Resources representatives and the Management. We are always here to support you as you develop your strengths, abilities and skills with us.

I wish you great success in your career with us. Welcome again!

Alice Wong
President

FOREWORD

This Staff Handbook sets out the main terms and conditions of employment offered by Imaginex Group ("the Company" or "Imaginex") for all permanent employees' reference and compliance. This Staff Handbook is incorporated into all employments of contract between Imaginex Group and its permanent employees.

Imaginex Group reserves the right to modify, alter, amend or remove the provisions of this Staff Handbook as circumstances may require. Employees will be advised of any alterations or changes through e-mails, circulars or the Intranet.

Matters not covered in this Staff Handbook shall be governed by the HK Employment Ordinance, other applicable ordinances and the contract of employment between the employee and Imaginex Group. In the event of any conflict between this Staff Handbook and the employee's contract of employment, the provisions of the contract of employment shall prevail.

This Staff Handbook shall be deemed to be made in Hong Kong and its validity, construction and performance shall be governed in all respects by the Laws of the Hong Kong Special Administrative Region of Mainland China

In case of discrepancy between the English and Chinese versions, the English version shall prevail.

If you have any query, please contact the Human Resources Department directly.

ABOUT IMAGINEX GROUP

Founded in 1992, Imaginex Group is China's first fashion, beauty and lifestyle brand management and distribution company with unrivalled coverage of market and channels. A pioneer of the region's luxury market, Imaginex Group was the first to introduce luxury brands such as Ferragamo, Gucci, Prada and Cartier to China more than 30 years ago.

Building luxury, designer and premium contemporary fashion, beauty and lifestyle businesses with an entrepreneurial approach and the passion of a brand owner, Imaginex Group represents international fashion brands including alice + olivia by Stacey Bendet, AllSaints, Brooks Brothers, Canada Goose, Club Monaco, Isabel Marant, Isaia, Kate Spade New York, Marc Jacobs, Paul Smith, sacai and Tory Burch. The portfolio also includes lifestyle and beauty brands including Apivita, Augustinus Bader, Aveda, Christian Louboutin Beauté, Editions de Parfums Frédéric Malle, Hermès Parfum and Beauté, Joyce Beauty, Kilian Paris, L'Artisan Parfumeur, Natura Bissé and Penhaligon's.

Imaginex Group creatively positions its brands, staying true to their DNA while ensuring local relevance, and leverages the company's market intelligence, robust infrastructure and partnership network to build critical mass. It offers multiple partnership formats for long-term growth in Greater China and South East Asia including joint ventures, franchise and wholesale distribution as well as management services. Its brand portfolio speaks to the luxury and designer customers while also appealing to the booming aspirational middle market.

Imaginex Group currently operates more than 510 points of sale across over 54 cities in Mainland China, Hong Kong SAR, Macau SAR, Taiwan China and South East Asia and has offices in Hong Kong SAR; Shanghai, Beijing, Macau SAR; Taipei and Singapore.

The Lane Crawford Joyce Group is Asia's premier fashion retail, brand management and distribution group, comprising of three distinct individual companies – iconic, luxury department store Lane Crawford; cutting edge fashion boutique Joyce; and fashion, beauty and lifestyle brand management and distribution business Imaginex Group.

The Group is led by Ms Jennifer Woo, Chairman and CEO. In April 2023, Jennifer was inducted into the World Retail Congress Hall of Fame as a global retail innovator.

The Lane Crawford Joyce Group works with more than **800 international fashion and lifestyle brands**. The Group operates luxury department stores and boutiques, freestanding branded stores, e-commerce and omni-channel operations.

The three companies form a collaborative partnership to provide international brands with a market entry and growth strategy for Greater China, leveraging various distribution models, while maintaining separate identities, areas of specialty, individual but complementary business models, and individual growth plans.

The Group currently operates more than **520 points of sale across over 50 cities** in Greater China and South East Asia, with a total retail space of more than **2,000,000 square feet**. As the sheer size and diversity of China presents many challenges to international brand entry and growth, The Lane Crawford Joyce Group is uniquely positioned to be brands' trusted partner for all of Greater China.

The Group has one of the largest premium customer bases in the region, with more than **1.5 million active luxury customers** on its database.

The Lane Crawford Joyce Group and its companies are recognised as international benchmarks for retail innovation and creativity, and a reference for the Greater China luxury market. The Group has won a number of international awards for store design, retail concept, visual merchandising and creative marketing campaigns, including the prestigious International Retailer of the Year Award awarded to Lane Crawford by the National Retail Federation headquartered in the US.

The Group employs more than **2,900 people** and is deeply invested in the training and personal development of its talent, offering a Retail Academy and Wellness platform for their development.

www.thelanecrawfordjoycegroup.com

The Lane Crawford Joyce Group is wholly owned by Mr Peter Woo Kwong-Ching. Mr Woo is the Executive Chairman of World International Capital Group overseeing the listed Wharf Real Estate Investment Company Limited and The Wharf (Holdings) Limited, which manages an expanding portfolio of retail, residential, commercial and hotel properties, as well as a port and logistics business in Hong Kong, mainland China and Singapore. **In mainland China, its assets spans across 15 cities**, and include the International Finance Squares in Changsha, Chengdu, Chongqing, Wuxi and Suzhou (phased opening in 2021) which will feature luxury retail, hospitality, Grade A offices and Service Apartments. Most recently the Group launched the five-star luxury hotel "The Murray Hong Kong", a Niccolo Hotel, transformed from an iconic landmark building in the heart of Hong Kong SAR.

HISTORY

Imaginex Group was founded with a vision to bring a touch of Western luxury to Mainland China. The X in the name signifies “the meeting point of luxury brands and customers”.

In the beginning, Imaginex Group started with only two brands, Elizabeth Arden and Salvatore Ferragamo, and a team of less than 20 employees. In 1993, Imaginex Group set up the first luxury department store, Maison Mode, in the region in Shanghai and opened the door to Mainland China for many of the world’s top and most famous fashion brands such as Salvatore Ferragamo, Prada and Gucci.

Our partnership with Salvatore Ferragamo spans many tears and the cooperation evolved into a Joint Venture in 2000. In the past years, we have brought a lot of international fashion and lifestyle brands to Greater China and South East Asia.

Milestones

1992
Born in Hong Kong

1993
Maison Mode opens in Shanghai, Mainland China’s first specialty store selling global luxury brands
Brings Prada, Gucci and other brands to Mainland China
First Salvatore Ferragamo flagship opens at the Mandarin Oriental Hotel Hong Kong

1994
First Salvatore Ferragamo store opens in Mainland China

1995
Expands and brings YSL and Mandarina Duck to Singapore

1996
Opens the first Cartier boutique in Mainland China

2000
Acquisition of Salvatore Ferragamo Hong Kong JV
Opens the first Paul & Shark store in Mainland China

2002
Takes over Hugo Boss from Lane Crawford
Acquisition of Ferragamo Taiwan JV
Sets up Taiwan office

2003
Opens first Coach store in Mainland China
Opens first Marc Jacobs store in Mainland China

2005
Opens first Tumi store in Mainland China

2006
Opens first Juicy Couture store in Hong Kong

2007
Acquisition of Bally JV
Sets up Singapore office

Milestones

2008
Opens first Club Monaco store in Hong Kong

2009
Opens first Jo Malone London store in Hong Kong

2011
Opens first 3.1 Philip Lim store in Hong Kong

2012
Takes over Paul Smith distribution in Hong Kong and Mainland China

2013
Opens first Paul Smith flagship store in Beijing
Opens first alice + olivia by Stacey Bendet store in Hong Kong
Sets to exceed 500 POS

2014
Opens first Scotch & Soda and Isaia store in Hong Kong

2015
Takes over Isabel Marant and DKNY distribution in Hong Kong
Takes over Tory Burch distribution in Taiwan

2016
Provides management service for ba&sh and Golden Goose Deluxe Brand in Hong Kong
Provides management service for AGNONA and Isaia in Mainland China

2017 - 2018
Provides management services for Tumi and Isaia
Walton Brown is integrated into Imaginex with Brooks Brothers
Kate Spade New York is added to Imaginex brand portfolio
Provides management services for Canada Goose in Hong Kong, Taiwan and Mainland China

2019
Apivita opens first store in Taipei

2020
Augustinus Bader opens first store in Taipei
Hermès Parfum and Beauté opens first store in Taipei

2021
Takes over sacai in Hong Kong
Joyce Beauty is transferred to Imaginex in Hong Kong
Kilian Paris and Editions de Parfums Frédéric Malle are transferred to Imaginex in Hong Kong
Provides management service for L'Artisan Parfumeur, Penhaligon's and Christian Louboutin Beauté in Mainland China

2022
AllSaints joins Imaginex in 2022 but was first present in Mainland China with TMall in 2017
Bimba Y Lola is first launched with TMALL
Opens first Vince store in Shanghai

2023
Provides management service for AllSaints in Mainland China

OUR VISION

Bringing passion, fashion, lifestyle and choice to Asia, our vision is to be the best brand builder in the region.

OUR MISSION

Our mission is to bring the world's fashion and lifestyle brands to Greater China & South East Asia. We forge long-term relationships with our partners based on mutual respect and shared passion. We build brands in Asia through creative positioning, innovative execution, and a deep understanding of what it takes to succeed in local markets. We deliver proven retail expertise supported by world-class infrastructure on the ground. Our success is based on providing quality, choice, and excellent service to all our customers across Asia.

OUR VALUES

Passion for Excellence

We believe in the drive to be the best that you can be

We believe in the entrepreneurial spirit. We celebrate those who actively seek out opportunities to continuously deliver results and improvement to our customers, our partners and our people. We admire those who devote their passion to our brands, unleash their creativity, inspire and motivate us all.

Willingness to Change and Innovate

We believe in the importance of creativity

We embrace the spirit of the pioneer. We learn, we grow, we lead changes and we think out of the box. Sometimes, things do not work out exactly as we planned: so we try again, we change our approach, and through perseverance and courage, we make new things happen.

Teamwork & Family Spirit

We believe in the power of people

We are one team working together for the good of our business, our customers, our partners and each other. We believe that with respect, love and fairness, we can achieve great things and help each other to achieve our potential in talented harmony.

Trust and Respect

We believe in honesty and integrity

Trusting and respecting each other are fundamentals. We believe in doing the right thing, no matter what the circumstances. We expect dignity, decency and a sense of justice to motivate every action that we take as individuals, and as a company.

HUMAN RESOURCES PRACTICE

People is key to the success of Imaginex and we strive to build and provide a workplace where all of our employees would be able to contribute their talent, exceed their potential, enjoy the work and feel being part of the big family. As a responsible employer, Imaginex upholds the principles of the following management practices:

Grow with the Company

We believe in a right match of attitude, skills and experience with the job requirement is the very first step to enable success for both Imaginex and the employees. Imaginex is keen to nurture its employees and provide support to facilitate employees performing to their best. All employees will be given opportunities to learn and grow with Imaginex through training, development programs, job rotations, special projects and the like to excel and progress.

Reward for Performance

We believe in rewarding for performance and recognising our employees through on the job exposure, training and development opportunities, salary increase and career progression. Employees are expected to contribute their best efforts according to the goals and objectives set for their respective work area.

Support our Core Values

We believe the criticality of employees exhibiting behaviours that supports Imaginex core values. All people related processes are aligned with the Company's values, aiming to reinforce and build the Imaginex culture. We also encourage open and transparent engagement with our staff through different communication channels such as staff newsletter, focus groups and survey etc.

Respect Privacy

We believe in respecting employees' privacy including the use of personal data and information. Imaginex will adhere strictly to applicable laws relating to privacy, including the Personal Data (Privacy) Ordinance, to ensure the collection, holding, processing or use of personal data of its employees are in compliance with applicable laws.

Promote Fairness

We believe in the importance of providing a fair working environment. Discrimination on grounds such as sex, marital status, family status, pregnancy, race and disability in the Company is definitely not tolerated. The Company will ensure that individuals are fairly treated under the process of recruitment, promotion, performance management, compensation, etc.

DEFINITIONS, INTERPRETATION AND GUIDANCE

I. Definitions

(a) **Applicable Law** means all the laws and regulations of the Hong Kong Special Administrative Region that apply to the Company and/or the employees, both generally and in respect of any particular provision of this Staff Handbook;

(b) **Business Partners** means the Company's goods or services suppliers, distributors, joint venture partners and companies, landlords/leaseholders, tenants/lessees and any other third parties with which the Company transacts business, excluding the Company's retail customers;

(c) **Department** means a department of the Company, such as the HR Department or the Finance Department;

(d) **employee** means a full-time or non full-time employee of the Company, unless otherwise expressly defined differently for a certain policy or provision in this handbook. We may also sometimes refer to employees as ''**staff**'' or ''**staff- member(s)**'';

(e) **Line Manager** means the person at the Company to whom you directly report in your day-to-day employment activities;

(f) **policy** means a policy in this Staff Handbook or any other policy approved by the Company that has been notified to its employees;

(g) **Related Parties** means the Company's employees, retail customers, Business Partners, agents, competitors and recruitment candidates;

(h) **termination** means the cessation of the employee's employment, including by resignation, retirement, the expiry of a fixed-term employment contract, redundancy, mutual agreement between the parties or dismissal of the employee in compliance with Applicable Law.

II. Interpretation

We have also set out below some interpretation rules to make the meaning of certain words and phrases in this Staff Handbook as clear as possible. In this Staff Handbook:

(a) headings are for convenience only and do not affect interpretation; and

(b) a reference to:

- a section, provision or Schedule, unless the context otherwise requires, is a reference to a section or provision of, or a Schedule to, this Staff Handbook;
- a sub-section means another portion of the same section as that within which the reference is contained;
- includes or including does not limit what else may be included;
- the singular includes the plural and vice versa (unless the context otherwise requires); and
- any word used in any gender-based form includes all genders.

III. Application of 'Applicable Law'

Each policy in this Staff Handbook is subject to Applicable Law. The policies should therefore be read as allowing the Company to apply them up to the maximum extent permitted by Applicable Law, but **not** any further than that. The Company cannot enforce any part of this Staff Handbook in a way that would breach any restrictions, limits, conditions or requirements imposed by Applicable Law. *For example*, any disciplinary action taken by the Company against an employee will always be subject to the limits of what Applicable Law allows the Company to do in this respect.

IV. Employee Obligations under Policies and Employment Contracts

Employees must comply both with the policies in this Staff Handbook **and** with any obligations set out in their employment contracts, terms and conditions of employment or other employment documentation.

V. Responsibility for communication, training and compliance in relation to the policies

Unless stated elsewhere in this Staff Handbook, the Human Resources Department is responsible for communicating awareness of these policies, for organising adequate training in relation to them and for enforcing the policies. All employees who have any other employee reporting to them (i.e. Line Managers) have a similar responsibility in respect of policy communication, training and compliance in relation to the employees who report to them. Most importantly, it is every employee's responsibility to read and understand these policies.

Some of our policies, such as our Anti-Corruption policy, must also be communicated to the Company's Business Partners and some other third parties. Unless otherwise stated in this Staff Handbook, the Company will be responsible for this communication.

VI. Raising concerns under the policies

Decisions as to what is acceptable behaviour at work, whether under these policies or otherwise, are not always easy. If any employee is in doubt as to whether a complaint should be made about any matter covered by these policies, the employee should discuss the matter with the employee's Line Manager or the Human Resources Department.

VII. Breach of the policies

An employee's failure to comply with these policies could result in the Company taking disciplinary action against the employee, up to and including summary dismissal. In some circumstances this could also lead to litigation proceedings and/or criminal prosecution under the provisions of Applicable Law.

VIII. Employees' acceptance of the policies

Please acknowledge your acceptance of these policies through the Company's online employee portal, the link to which has been shared with you by the Company.

PART A: POLICIES SPECIFIC TO IMAGINEX GROUP

1. EMPLOYMENT

1.1 Hiring

Please note: this Hiring section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

All employees are engaged under a written contract of employment with the Company. The contract period (if applicable), remuneration package, working hours, annual leave, benefits and termination provisions are specified in the contract.

New employees shall complete the new joiner procedures within the first week and provide all required information.

No employee may engage in outside activities which may conflict directly or indirectly with the Company's interests, without the prior written permission of the Company.

1.2 Probation

Please note: this Probation section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

All permanent employees are required to undergo a probationary period, unless otherwise specified in the contract of employment. Subject to the Management's discretion, the probationary period may be shortened or extended. If the probation is extended, the employee will be informed in writing with reasons for the extension of probation. A review meeting between the employee and his/her Line Manager may also be conducted. Upon successful completion of the probationary period, permanent employment will be confirmed in writing.

1.3 Transfer and Secondment

An employee may be transferred from one department to another, one branch to another or from one job to another, on temporary or permanent basis, as may be required to suit operational needs. Prior to such transfer, an employee will be advised in advance in writing with details of the arrangement and the reasons for the transfer.

1.4 Termination of Employment

Please note: this Termination of Employment section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

The employment may be terminated, either by the Company or the employee, by giving the stipulated period of notice in writing, or payment in lieu, as specified in each individual employment contract.

If an employee is absent from work for three consecutive days without legitimate reasons or notification, the Company may regard that as abandonment of employment. On a case by case basis, the Company may regard the employee as having terminated the contract and may require the employee to observe the provisions of the termination clause of the employment contract. The Company reserves the right to take appropriate legal actions whenever necessary.

(a) Payment in lieu of Notice

Should an employee fail to give the stipulated notice period or payment in lieu to terminate their employment this will constitute a breach of contract. The Company reserves the right to take appropriate actions to resolve any dispute or to enforce its legal rights.

(b) Summary Dismissal

The Company reserves the right to summarily dismiss any employee without notice or payment in lieu of notice under the following circumstances:

(i) If the employee in relation to his/her employment:

- wilfully disobeys a lawful and reasonable order;
- is found guilty of any gross misconduct or wilful neglect in the discharge of the specified duties;
- is found guilty of fraud or dishonesty;
- commits an act which, in the opinion of the Company brings or could bring the employee or the Company into disrepute;
- has been convicted of any criminal offence other than an offence which in the reasonable opinion of the Company does not affect this appointment; or

(ii) On any other ground on which the Imaginex Group would be entitled to terminate the contract of employment without notice under Common Law.

Any delay by the Company in exercising its right to summarily dismiss an employee in these circumstances shall not prejudice its right to do so.

On leaving the Imaginex Group, employees are not entitled to keep and are required to return to the Company all properties, proprietary information/documents issued/provided to them during their service with the Company (e.g. staff identity card, access card, keys, medical cards, uniform, Staff Handbook, office equipment, confidential information, etc.). Employees are not allowed to keep any unauthorised copies in any form of the Company's properties or documents. In addition, employees are not allowed to send group emails within the Company or send emails to any third parties outside the Company with respect to the departure without the consent of the Company.

Imaginex Group shall be entitled at any time during employment, or upon termination, to deduct from salary any monies due from the employee to the Company including but not limited to any outstanding loans, advance, training cost, cost of repairing any damage or loss of the Company's property caused by the employee (and of recovering the same) and any other monies owed by the employee to the Company subject always to the Employment Ordinance and/or mutual agreement.

1.5 Retirement

The normal retirement age of the Company is 60. The Company may at its full discretion, hire a retired employee or engage a retired employee for contract for service after the normal retirement age.

1.6 Certification of Employment

Where necessary, an employee may apply for a certification on salary, duties and duration of employment with the Imaginex Group.

The employee should submit a form of "Company Letters" to the Human Resources Department specifying details of the purpose, information needed, and the addressee, etc. Employees may download the application form from i-jam.

2. WORKING HOURS

Please note: this Working Hours section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

Employees will be individually advised of their respective working hours according to the operations and requirements of their departments.

The Company reserves the right to alter the normal working hours, rest period and pattern of normal working hours whenever necessary.

2.1 Overtime/Time Off

Only certain frontline positions are eligible for overtime compensation in the form of time off in lieu. Employees may refer to the Human Resources Department for their eligibility of overtime compensation.

Overtime payment is calculated as per the prevailing policy in force, which is subject to change from time to time.

3. COMPENSATION AND BENEFITS

3.1 Salary

Salaries will be paid on the last weekday of every calendar month. Should that day fall on a public holiday, early salary release on the preceding working day will be arranged. An electronic pay slip will be issued to individual employees with breakdown of salary payment and items of deduction for the month. Employees may check with the Human Resources Department directly for clarifications.

3.2 Annual Bonus

At the sole discretion of the Company a bonus may be payable to eligible employees based on overall Company business results and individual performance for that bonus year; and the achievement of any performance targets set by the Company. Should the Company decide that a bonus may be payable to employees, the Company will elect a period of 12 consecutive months as the bonus payment period. Should an employee join the Company part-way through the said payment period, any bonus will be calculated pro-rata for every completed calendar day. Eligibility for a bonus will cease should the employee resign from the employment or be terminated by the Company, on or prior to the relevant bonus payment date. The amount of any bonus will be determined by the Company in its absolute discretion and subject to such performance factors and other conditions as the Company may determine. Payment of a bonus in one year does not give rise to any entitlement in a future year.

3.3 Annual Salary Review

Salary review is conducted annually. Salary adjustment is determined with reference to the performance of the individual and the business as well as market pay practices and trends. Depending on the review results, salary may be adjusted upward, downward or remain unchanged. Annual salary review does not apply to employees who are under probation or have tendered their resignation.

3.4 Sales Commission/Incentives

Store-based employees who are responsible for achieving the Company's sales targets are eligible to participate in the Company's Sales Commission/Incentive Scheme. Details of the scheme will be provided to the eligible employees.

The Company reserves the right to change the Sales Commission/Incentive Scheme without prior notice.

3.5 Employee Compensation

(a) Definition

'Employee' for the purposes of the Employees' Compensation Ordinance is 'any person who has entered into or works under a contract of service or apprenticeship with an employer in any employment whether by way of manual labour, clerical work or otherwise and whether the contract is expressed or implied, in oral or in writing'.

(b) General

All employees are expected to play an active role in accident prevention and report all accidents, dangerous acts or conditions to the Line Manager immediately.

(c) Insurance

All employees are insured by the Company against accidental injury incurred on normal duty which is deemed to arise out of and in the course of employment.

(d) Procedures

If any employee suffers from injury, the accident should be reported immediately to the Business Unit/Function Head and the Human Resources Department. Whether the injury is serious and an ambulance is called for, or minor injury occurs, it is advisable that a colleague (ideally Line Manager) must accompany the injured employee to consult a registered doctor or go to a hospital for medical treatment.

(i) If an employee suffers from injury in an accident arising out of and in the course of his/her employment, it is treated as a work injury and not counted as normal Sick Leave. However, the employee should submit Sick Leave Certificate(s) and keep the Business Unit/Function Head/Line Manager concerned as well as the Human Resources Department informed as to the date they will return to work.

(ii) The employee should seek medical examination or treatment by either a government doctor or a private registered doctor.

(iii) The employee should submit the Sick Leave Certificate(s) to his/her Line Manager as soon as possible and keep one photocopy for himself/herself. He/She should visit his/her medical advisor regularly to obtain continuation medical certificates and when he/she is fit to resume his/her normal duties, a final clearance certificate should be obtained.

(iv) During the Injury Leave, the employee may receive the following compensation from the Company before the medical assessment is completed.

- Medical expenses: These include costs for out-patient treatment or hospitalisation subject to the provisions of the relevant legislation from time to time. After the employee has paid the medical expenses, he/she should give the receipts to the Human Resources Department for reimbursement.

- Salary: The employee is entitled to four-fifths of his/her normal wages during the Injury Leave period.

(v) If the sick leave exceeds seven days, the employee will receive from the Labour Department a Medical Clearance Form together with a written advice on procedures for medical assessment. He/she must follow the advice and attend the medical assessment because it is a vital step for determining the amount of compensation.

(vi) For details on the method of calculating compensation, the employee may approach the Human Resources Department for assistance.

3.6 Medical & Dental Schemes

Upon successful completion of the probationary period, certain permanent employees will be entitled to the Company's medical and dental schemes. The Company reserves the right to change the benefits coverage as the Company deems fit and appropriate. Benefits will be provided in accordance with the agreement made between the Company and the service providers. In case of inconsistency, the scheme document shall prevail.

For enquiries, please contact the Human Resources Department.

3.7 Pension

All eligible employees will participate in the Mandatory Provident Fund Scheme (MPF) in accordance with the provisions of the Mandatory Provident Fund Schemes Ordinance and the Trust Deed and Rules of the Scheme. For more details, please refer to the "MPF Guidelines" and "MPF Booklet" or contact the Human Resources Department.

3.8 Business Travel Insurance

This insurance is designed to apply to all accidents sustained by employee while travelling on Company business anywhere in the world. An employee is required to notify the Administration Department prior to the trip in order to obtain a travel insurance card and to assure coverage.

3.9 Employee Purchase Privilege

(a) Eligible Members

Unless otherwise stated in the employment contracts, permanent employees are eligible to employee discount upon completion of at least 3 months service and issuance of a staff card with photo properly affixed.

(b) Terms and Conditions of Employees Purchase

Eligible members are only allowed to make purchases from Imaginex Group-designated standalone stores in Hong Kong for their personal use.

Products purchased through this privilege should not be resold.

Any abuse of employee discount benefits will result in:

- immediate cessation of such benefits without prior notice; and/or
- refund by the employee of the difference between retail price and employee discount price; and/or
- other disciplinary actions including but not limited to termination of employment.

(c) Identification

Eligible employees are required to make purchases in person and are required to present his/her staff card. Failure to present a valid staff card will result in purchases being charged at the full retail price.

The Company has absolute discretion to decline any employee purchase in case of doubt of identification.

(d) Discount Rate and Payment Method

For the prevailing discount rates and purchase limit, please refer to the IMX Station /i-jam.

Payment must be settled by the eligible member in person and by using the personal credit card/ EPS or cash.

(e) Applicable Merchandise

Employee discounts are applicable to selected brands and merchandise and are subject to change without prior notice. Employees are encouraged to check with the sales staff before making purchases.

(f) Other Conditions

Employees are not allowed to perform shopping during their duty hours unless otherwise approved by the Business Units/Business Unit/Function Head.

Employee discounts cannot be used in conjunction with other promotional offers and Imaginex Customer Loyalty Program.

The Company has the sole discretion to withdraw the Employee Purchase Privileges without any prior notice or to change the discount rates and/or terms and conditions as it deems fit from time to time.

4. HOLIDAYS AND LEAVE

4.1 Annual Leave

Please note: this Annual Leave section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

All employees who have been employed by the Company under a continuous contract as stipulated in the Employment Ordinance are entitled to annual leave with pay. Employees are eligible to apply for annual leave with pay after completion of probation or 3 months of service, whichever is earlier. In general, annual leave entitlement will be based on the employees' job grade and years of service.

(a) Annual leave entitlement is calculated on a calendar year basis. Employees with less than one year of service or who have resigned or are terminated (excluding summarily dismissed) by the Company before 31st December but with at least 3 months' service during the calendar year will be entitled to pro-rata annual leave based on number of days served.

(b) Annual leave shall be taken in each year at such time or times as approved by the employee's Line Manager and must be cleared every year. Employees are deemed to take their statutory annual leave before their contractual annual leave. Except for employees who join the Company on or after 1 August in any given year, unused annual leave may not normally be allowed to be carried forward to the following year unless special approval has been obtained from the respective Business Unit/ Function Head/ Senior Management Team. Once approved, the unused annual leave must be used by 31 March of the following year.

(c) Exception: Store-based employees are advised not to take annual leave during peak season/periods. Business Unit/Function Heads will specify the requirements based on operational needs.

(d) An employee, upon leaving the Imaginex Group, will be granted payment in lieu of unused annual leave, if any.

4.2 Statutory/Public Holidays

All full-time employees (office and frontline) are entitled to public holidays with pay. For part-time positions, unless otherwise stated, employees are entitled to statutory holidays with pay in accordance with the provisions of the Employment Ordinance. Employees who are required to work on statutory/public holidays will be granted compensation leave (see below) in lieu of the statutory/public holidays.

4.3 Rest Days

For office employees, statutory rest day falls on Sunday. For employees who perform shift duties, rest days will be arranged in accordance with the rosters approved by Business Unit/ Function Heads /authorised persons.

Employees who are required to work overseas outside normal working hours will be entitled to one rest day if they have worked continuously for a period of not less than six days.

In case of emergency and/or operational needs, an employee may be required to work on his/her rest day. In this case, a Compensation Leave will be granted.

4.4 Birthday Leave

All full-time permanent employees are entitled to one working day of birthday leave with pay after completion of probation. Birthday leave should be taken within the birthday month. Any unused birthday leave will be forfeited and no payment in lieu will be granted upon leaving service of the Company. Employees who have submitted resignation are not eligible to birthday leave.

Birthday leave is granted on a discretionary basis and does not form part of the terms and conditions of employment. The Company reserves the right to amend this benefit from time to time.

4.5 Anniversary Leave

Full-time permanent employees upon completion of one year of service are entitled to one day of paid anniversary leave.

Anniversary leave shall be taken within 30 days from the employee's service anniversary day. Unused anniversary leave will not be allowed to be carried forward to the following year and there will be no payment in lieu of unused anniversary leave.

Application for anniversary leave should be submitted to the designated manager at least one calendar week in advance.

Employees who have submitted resignation are not eligible to anniversary leave.

4.6 Sick Leave

All employees who are unable to perform their normal duties by reason of ill-health will be granted sick leave under the following criteria. Sick leave and sickness allowance entitlements are subject to the provisions of any applicable legislation, as amended from time to time.

(a) Frontline Employees

Frontline employees who are unable to attend work should inform their Line Manager, Business Unit/Function Head or shop manager by phone, or email two hours prior to the start of their working day to arrange replacement cover. Should the Line Manager be not available, the Human Resources Department should be informed. Frontline employees who have completed probation are entitled to full pay sick leave for sick leave period of less than 4 consecutive days at the discretion of brand heads. For sick leave period of 4 days or above, paid sick leave will be granted in accordance with the provisions of the labour legislation currently in force.

(b) Office Employees

Office employees who are unable to attend work should inform their Line Manager of any absence by phone or email within 30 minutes of the start of their working day (or as soon as possible thereafter). Should the Line Manager be not available, the Human Resources Department should be informed. For the first three months of employment, paid sick leave will be granted in accordance with the provisions of the labour legislation currently in force. From the fourth month onwards, full paid sick leave will be granted for the entire period taken provided that the number of sickness days is within the accumulated sickness allowance under the Employment Ordinance.

(c) Sick Leave Certificate

All employees are required to produce a sick leave certificate from a registered medical practitioner to substantiate their absence from duties after they resume work. Please be reminded that a certificate of attendance will not be accepted as sick leave certificate. Failure to submit a valid sick leave certificate shall be regarded as a deliberate absence from work and no sick leave will be granted.

(d) Sickness Allowance during Resignation Notice Period

During resignation notice period, paid sick leave will be granted in accordance to the prevailing labour legislation. The Company reserves the right to change the sick leave payment policy.

4.7 Compensation Leave

Office employee will be entitled to compensation leave in the following situations:

(a) If reporting for duty on Saturday, Sunday and/or public holidays for business events such as road show, bargain sale, marketing events or stock take, training, (leisure or events of an entertainment nature are excluded).

(b) If working overseas on Saturday and/or Sunday during business trips.

(c) If public holiday(s) fall(s) within business trips.

(i) Conditions:

- (a) and (b)/(c) are mutually exclusive.
- Prior approval from Business Unit/ Function Head is required for situation (a).
- Compensation Leave should be taken within 60 days after the original public holiday/working Saturday/working Sunday, or it will be forfeited.
- Under no circumstances will payment in lieu be made for the compensation leave.
- Should there be any dispute on any issues relating to the compensation leave, the decision of Management is final.

4.8 Marriage Leave

Upon completion of one year of service, full-time permanent employees are entitled to 5 working days of paid marriage leave. Employees who have completed their probation but with less than one year of service are entitled to a pro-rata paid marriage leave subject to the number of completed months of work. Employees who have submitted resignation are not eligible to marriage leave.

Marriage leave should be taken within one calendar year from the registered date of marriage. Unused marriage leave will be forfeited. The Company will only grant marriage leave once to the eligible employees during their employment with the Company.

Employee is required to provide the marriage certificate within one month after the marriage leave.

4.9 Maternity Leave

Full-time permanent female employees who have served 40 weeks of continuous employment with the Company immediately before the commencement of scheduled maternity leave are entitled to 14 weeks of maternity leave with full pay. If the female employee has served less than 40 weeks of service with the Company, 14 weeks of maternity leave will be granted on an unpaid basis.

The pregnant employee should inform the Human Resources Department about her pregnancy as soon as possible and at least 12 weeks before the expected date of confinement. A medical certificate issued by a registered medical practitioner should be provided.

Office employees are entitled to 100% basic pay during the authorized maternity leave. Whereas frontline employees are entitled to 100% of the average daily wages of the past 12 months preceding the first day of the maternity leave. If a frontline employee is employed for less than 12 months, the calculation shall be based on the shorter period.

The pregnant employee may commence her maternity leave 2-4 weeks before the expected date of confinement. The employee should inform the Human Resources Department within 7 days of her confinement.

The Company will grant sick leave for medical examination in relation to pregnancy, post confinement medical treatment or miscarriage supported by an appropriate medical certificate. A certificate of attendance issued by a registered medical practitioner, a registered Chinese medicine practitioner, a registered midwife or a registered nurse can be regarded as an appropriate medical certificate for a medical examination in relation to pregnancy.

Maternity plus (M+) leave is available on a voluntary basis to female employees to recognise the need to have more time away from work to recover from maternity leave following the birth.

The female employee is eligible for 10 working days with 50% pay. M+ Leave must be completed within 12 months of the actual date of birth. Earned annual leave and unpaid leave may be taken to extend the leave with the approval of respective Business Unit / Function Head.

Other employment should not be undertaken during maternity leave.

4.10 Paternity Leave

A full-time permanent male employee is entitled to 10 days' paternity leave for each confinement of his spouse/partner if he is the father of a new-born child or a father-to-be; has been employed under a continuous contract and has given the required notification to the employer.

The male employee may take paternity leave at any time during the period from 4 weeks before the expected date of delivery of the child to 14 weeks beginning on the actual date of delivery of the child. The employee may take all 10 days of paternity leave in one go or on separate days.

A male employee is entitled to paid paternity leave if he has been employed under a continuous contract for not less than 40 weeks immediately before the day of paternity leave and has provided the required document such as birth certificate to the employer within the period as required by the labour legislation.

For a male employee who has completed his probation but has been employed under a continuous contract for less than 40 weeks immediately before the day of paternity leave and has provided the required document such as birth certificate to the employer within the period as required by the labour legislation, he will be entitled to a pro rata paid paternity leave subject to the number of completed months of work.

4.11 Adoption Leave

Intent

This is a policy to govern adoption leave which is applicable to Imaginex Group's permanent full-time employees. It covers two (2) types of adoption, local adoption within Hong Kong and non-local adoption outside Hong Kong.

(a) General Conditions

Eligibility

Adoption leave is available to Imaginex Group's employees as follows:

- The eligible employee is a permanent full-time staff member, and
- Is adopting a child under the age of 16 and will be the prime carer, and
- Employee who is a member of a couple/domestic partnership/registered partnership where adoption jointly.[1]

(b) Administration of Leave Management and Payroll Operation

(i) An eligible employee with less than 40 weeks of continuous employment with the company immediately before the commencement of their adoption leave and having given notice to the employer is entitled to non-paid adoption leave.

(ii) An eligible employee with 40 weeks of continuous employment with the company immediately before the commencement of adoption leave and having properly given notice to the employer is entitled to paid adoption leave.

(iii) Only one period of leave will be available to employee irrespective of whether more than one child is adopted at the same time.

(iv) An Employee will not qualify for adoption leave (whether paid and non-paid) if he/she:

- Becomes a special guardian or kinship carer
- Adopts a family member or stepchild
- Has a child through surrogacy
- Adopts privately without permission from the Local Authority or approved adoption agency.

(v) During the approved adoption leave period, an employee is entitled to four-fifths of the employee's average wages.

[1]Only one (1) member of the couple can entitle to Adoption Leave, and the couple may choose which partner takes Adoption Leave.

(c) Types of Adoption Leave

(i) Local Adoption Within Hong Kong - Entitlement

The employee is entitled to a continuous period of adoption leave according to the following qualifier based on the age of the adopted child:

AGE of THE ADOPTED CHILD	LENGTH of ADOPTION LEAVE
0 – 3 years old	Up to 10 weeks
3+ – 6 years old	Up to 8 weeks
6+ – 12 years old	Up to 6 weeks
12+ – 16 years old	Up to 4 weeks

With the agreement of the employer, an adoptive employee may decide to commence their adoption leave on:

- The actual date of the child's placement, or
- A predetermined date that is no earlier than 14 calendar days before the expected date of placement.

If an employee wishes to return to work before the end of the original adoption leave period specified, the employee must inform their Line Manager/Business Unit/ Function Head in writing, with a copy to the Human Resources Department, confirming the date he/she wishes to return.

- The employee who has specified to take not less than eight weeks of leave must give at least three weeks' notice, or
- The employee who has specified to take less than six weeks of leave must give at least two weeks' notice.
- Any rest days, sick leave or holidays that fall into the adoption leave period shall be counted as part of the adoption leave.

Adoption leave is applicable to new adoption cases and no maternity leave, maternity leave plus or paternity leave has been claimed in the name of it.

Notice and Records re Local Adoption Leave

The employee must give written notice of their intention to take adoption leave to their Business Unit/ Function Head and the Human Resources Department within 5 days of being matched with a child, AND not less than 1 month before their intended start date, along with the submission of their matching certificate.

The employee must specify the following when giving notice of their intention to take adoption leave:

- The length of leave period they wish to take (maximum to the assigned length of adoption leave), and
- The leave start date, and
- The date of the child's placement.

If for any reason the start date of the adoption leaves change, the employee must give at least 5 working days' notice of the change.

(ii) Non-local Adoption Outside Hong Kong - Entitlement

Same conditions apply as for domestic adoption, with the following exception:

With the agreement of the employer, an adoptive employee may decide to commence their adoption leave on:

- The date of the child's placement, and
- A predetermined date that is no earlier than 14 calendar days before the expected date of placement.

Notice and Records re Non-local Adoption Leave

The employee must give written notice of their intention to take adoption leave to their Business Unit/ Function Head and the Human Resources Department at least 14 calendar days before the expected date of the child's arrival into the country, along with the submission of their matching certificate.

The employee must specify the following when giving notice of their intention to take adoption leave:

- The length of leave period they wish to take (maximum to the assigned length of adoption leave), and
- The leave start date, and
- The expected arrival date of the child into the country, and
- The expected date of the child's placement.

If for any reason the start date of the adoption leaves change, the employee must give notice of the change within 3 days after the date the child enters the country.

4.12 Compassionate Leave

The Company will grant paid compassionate leave on the bereavement of immediate family members. Immediate family members include:

- Spouse
- Children
- Parents
- Brothers
- Sisters
- Parents-in-law
- Grandparents

Full-time Permanent employees will be granted a maximum of 2 consecutive days for funeral taking place in Hong Kong, or a maximum of 3 consecutive days for the funeral taking place outside Hong Kong. Full-time Permanent employees are entitled to compassionate leave from their start dates of employment.

4.13 Examination Leave

Full-time Permanent employees may apply for examination leave for attending examination(s) in relation to course(s) that are sponsored by the Company or where professional qualifications are required for the discharge of individual's duties. In the latter case, the examination must be held by recognised, accredited professional authorities, such as ACCA, HKICPA etc. A maximum of 3 days paid examination leave per year will be granted on the date (or half day) when the examination(s) is held. Should the examination fall on a Saturday, Sunday, rest day or public holiday, no examination leave will be granted.

4.14 Jury Service Leave

If employees are selected to perform jury service at the court's request, the Company will grant jury service leave with pay to employees upon receipt of the official notification/document issued by the Registrar of the High Court or Coroner's Court.

4.15 Unpaid Leave

It is at the Company's sole discretion to grant unpaid leave to employees on condition that their annual leaves are exhausted and with a justified reason. Application of unpaid leave will be considered on a case by case basis. Line managers are required to notify the Human Resources Department on all unpaid leave applications for payroll purpose.

Unpaid leave application of more than 14 days must be approved by a member of the Senior Management Team members and the Human Resources Department.

Benefits for employees who are on unpaid leave for six consecutive months or more will be affected. Employees are advised to contact the Human Resources Department for details.

4.16 Leave Application

Should an employee intend to apply for any of the above leave, application should be made via the e-Leave system with supporting documents, e.g. sick leave certificate, marriage certificate, and submit these to your Line Manager for approval. All leave will be counted in half-day or one-day. Annual leave, marriage leave and adoption leave should be applied for at least one month in advance except for special circumstances. Changes to approved leave must be made prior to the start of the leave period.

For login to the leave system, please visit IMX Station.

5. PEOPLE DEVELOPMENT

Passion for Excellence and Willingness to Change & Innovate are our Company's values. In line with the values to support and develop highly competent and motivated workforce, fully committed to achieving business objectives, the Company puts a strong emphasis on people development. The Company will systematically identify development needs, provide learning solutions and conduct regular assessments with employee according to the Company's established Performance Management System and Learning & Development Tools.

5.1 Performance Management System

Objectives setting and performance appraisal is an integral part of the Company's Performance Management System. The purpose of objectives setting is to align the goals and objectives of individual employee with the broader goals of the business so as to support and facilitate the achievement of the Company's business goals. The objectives and measurements agreed upon by appraisers and employees at the beginning of the review period will be used as the yardstick to objectively discuss, monitor and assess performance of the employee throughout the review period.

Performance appraisal process is an important means of reviewing an employee's achievements and key assessment elements throughout the review period. It covers the following aspects:

- how effectively the agreed objectives/targets have been achieved;

- assessment of an employee's performance on predefined elements.

Performance appraisal also provides an opportunity for employees to discuss their development needs and personal development plan with their appraisers so as to encourage continuous self-development.

Please visit IMX Station for login to e-PMS system for all office employees.

5.2 Learning & Development

The responsibility for personal development lies first with the individual and secondly with the individual's Line Manager. The Company offers both internal and external learning and development opportunities to enable our employees to continuously enhance individual capabilities and in turn contribute to the overall organisation performance.

The Learning & Development Department designs and conducts a wide spectrum of core workshops and development programmes to facilitate their career within the Company. All employees must attend the workshop(s) which is/are assigned to them. Apart from core workshops, learning and development can also be achieved by different tools such as, on the job training, project involvement and exposure, functional expertise training, self-study, role modelling, coaching and mentoring etc.

If an employee, out of his/her own initiative, elects to attend external courses relevant to his/her job duties or general course of continuing education, the Company may sponsor part of the course fee provided that such sponsorship has been approved by Business Unit/Function Head and the Learning & Development Department prior to the enrolment of the course and the employee has met the requirements as per the Policy of External Training Sponsorship. Details of the Policy can be found on i-jam.

5.3 Continuous Training

If a performance gap is identified due to the insufficiency of knowledge and skills of an employee to perform his/her job functions, the employee may be required to attend Continuous Training. During the training period, special job arrangements may be implemented with corresponding adjustments in salary. The Company will review the employment of the relevant employee in light of the Continuous Training results.

6. RULES & REGULATIONS

Please note: this Rules & Regulations section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

6.1 Attendance

As a general guideline, office employees who are unable to report to work due to sickness or personal reasons are required to notify his/her Line Manager within 30 minutes from their starting hour of work and store-based employees are required to report to his/her Line Manager two hours from their starting hour of work (please refer to the Sick Leave policy earlier in this Staff Handbook for further details). If employees are required to leave the office premises during working hours due to sickness or personal reasons, prior approval from the Line Manager or his/her designate is required.

Failure by an employee to notify his/her Line Manager or his/her designate on their absence from work will be considered as an act of serious misconduct and will be subject to disciplinary actions. Failure by an employee to attend work for three consecutive working days without authorisation will be considered as abandonment or a wrongful termination of employment and the employment contract may be terminated with immediate effect. The Company reserves the right to claim the employee for the payment in lieu of notice and other damages for wrongful termination of employment.

(a) Attendance Record Mechanism

All employees must be punctual in reporting for work. Persistent lateness or early departure is considered misconduct and will result in disciplinary action.

As and when required, employees shall work overtime per their Line Managers' arrangement.

Mechanisms enforced include the following:

(i) Access control log

Employees may be given access cards to record their attendance by touching their card on the card reader.

(ii) Attendance system

Employees shall log in and log out of the attendance system in person to record their attendance.
Employees shall clock in and clock out in person when reporting for duty, leaving work or under any other circumstances instructed by their Line Manager.

Prior approval from the Department Manager should be sought before working outside of the normal workplace due to job needs.

Enquires from the Human Resources Department on attendance records should be answered as soon as possible and in any case within two days. Otherwise, the employee will be treated as having been absent.

In case of doubt, please consult the Business Unit/Function Head/the Human Resources Department.

6.2 Business Cards

Permanent employees at Assistant Manager or above grade may ask for business cards bearing Company's name and logo, subject to the operational needs. Details can be referred to the "Business Card & Printed Matters Guideline".

6.3 Telephones

Employees are discouraged from using the telephone system for personal calls. Conversations must be kept to a minimum. Business calls must be given priority. Employees are prohibited from using the telephone system for personal long-distance calls. Employees breaching this rule will be subject to disciplinary action as well as liable to the charges of the long-distance calls plus handling fee of each call.

6.4 Mail

All mail must be addressed to the Company and not to individual employees.

Employees who have been in the habit of having personal mail addressed c/o the Company or the Company's Post Office Box, run the risk of having such mail opened as business mail.

An employee's personal mail should be sent to his/her home / personal correspondence address.

7. HANDLING OF COMPANY ASSETS

The Company strictly prohibits the unauthorised taking or re-selling of Company assets, including merchandise, packaging materials and brand souvenirs, etc.

7.1 Company Files and Accounts

The Company strictly prohibits falsifying documents or providing false accounts, which are legislative offences.

7.2 Use of Office Equipment and Other Company's Resources

Employees must at all times exercise care in using office equipment such as photocopiers, computers, printers, mobile phones, fax machines etc. These are the property of the Company. The use of office equipment and other Company's resources including, but not limited to, photocopiers, printers, email/internet facilities, etc. are provided for business use only.

7.3 Refreshment

Store-based employees should only eat and drink at designated places. Eating at the sale area is prohibited.

7.4 Name Badge

All employees who will directly serve customers should wear their name badges. Loss of a name badge should be reported to arrange re-issuance. It is forbidden to wear the name badge of other employees. Upon departure, the name badge should be returned to the Company. For loss of or not returning the name badge, a compensation fee of HK$100 is required to be made by the employee.

7.5 Lost Property

In the first instance, all lost property will be handed over to the Business Unit/Function Head or Store in-charge, together with details of the background circumstances. The Company will endeavour to trace owners of lost property via direct contact. If that method fails, the Police will be informed.

8. COMMUNICATIONS/EMPLOYEE RELATIONS

8.1 Staff Recreation Committee

All employees are encouraged to participate in the activities organised by the Company.

The Company will support such activities including but not limited to providing subsidies as appropriate.

8.2 Press Articles

Employees must not submit to the press, articles dealing with the Company's business interest, or the Company's conditions of service, without receiving prior permission from the Management. In the event if such permission is given, all matters for publication will be routed through the Management.

8.3 Photography Policy at One Island South

To control the usage of the images of our workplace at One Island South (OIS), it is the policy of Lane Crawford Joyce Group (LCJG) that prior approval must be obtained from the Group's Corporate Communications Department (GCC) for any photography taken by media, designers, visitors and any external parties. GCC has an archive of images that they have commissioned. If any employee wishes to use these images, please contact GCC.

For any third parties' request for images of our workplace, please direct them to GCC.

8.4 Disciplinary Action and Suspension

(a) Guiding Principle

The Company strongly believes that employee engagement comes from personal responsibility, passion and determination, not the fear of disciplinary actions. Employees should proactively understand the work standards that are expected of them and comply with all applicable rules and regulations. It should be understood that the disciplinary mechanism is for correctional purposes, not to punish individuals without reason. In case an employee would like to know more about the regulations, please approach the Department Manager or the Human Resources Department.

(b) Disciplinary Action and Suspension

(i) Policy

In order to achieve and maintain operational efficiency, it is essential that all employees should comply with acceptable standards of conduct. Disciplinary regulations are laid down with the objective of protecting the best interests of the Company and its employees.

(ii) Procedures

Disciplinary action against an employee may be taken in any of the following ways:

- Verbal warning

  An employee may be given a verbal warning in the first instance or instances of minor breaches. Line Manager should verbally discuss with the employee's unacceptable performance/behaviour in order to give the employee an opportunity to correct the behaviour or show improvement.

- Written warning

  An employee may be given a written reprimand in the first instance of more serious breaches or after repeated minor breaches for which verbal warnings have been given. All written warnings issued to an employee will state the particulars of the breach. It will be explained and interpreted clearly by the Business Unit/Function Head/Line Manager in the presence of the Human Resources Manager. The signature of the employee being served a warning is expected as an acknowledgement of such notice though it is not compulsory. The employee may explain himself/ herself in writing if he/she disagrees with the warning. The written warning will then be kept in the employee's personal file.

- Suspension without pay and/or staff benefits

  An employee may be suspended from duty with or without pay and/or his/her employee benefits if any of the following apply:

  - serious misconduct or persistent breaches of Company's rules and regulations;
  - pending an investigation by the Company; or
  - when criminal proceedings have been instituted against the employee.

  Except when criminal proceedings have been instituted against the employee, the maximum period of suspension normally will not exceed 14 days.

  The investigation by the Company will be concluded as soon as possible, within a reasonable time limit, and not later than the conclusion of any criminal proceedings (where applicable).

- Dismissal

  Any employee may be dismissed in case of serious misconduct or persistent breaches of Company's rules and regulations or conviction of criminal offence which in the opinion of the Management affects the employee's position in the Company. Please refer to the provisions earlier in this manual relating to termination of employment.

PART B: GENERAL POLICIES ACROSS ALL LANE CRAWFORD JOYCE GROUP COMPANIES

INTRODUCTION

I. The Purpose of this Part B of the Handbook

In this Part B of the handbook, we have compiled the main policies of the Lane Crawford Joyce Group that are not specific to a particular company or business. Instead, these policies apply across the entire Lane Crawford Joyce Group in Hong Kong, regardless of which company an employee works for.

As with Part A of this handbook, each section in this Part B of the handbook contains a separate policy. The policies reflect many of the principles of the Lane Crawford Joyce Group, including:

- ensuring a fair and respectful working environment;
- acting with integrity across our entire organisation;
- respecting confidentiality, intellectual property and data privacy; and
- working together to protect the Group and its assets.

Each set of policies in this part of the handbook begins with a short statement of the **principles** that those set of policies represent. The policies are then designed to help the Lane Crawford Joyce Group and its employees demonstrate these principles during their day-to-day working relationship.

Please note that, as with the company-specific policies contained in Part A of this handbook, a breach by an employee of these Group policies may result in the Company taking disciplinary action against that employee, up to and potentially including termination of the employee's employment.

In addition to these Group policies and the company-specific policies in Part A, some Departments have their own operational or other policies ("**Department Policies**"). These will be explained to relevant new hires at the appropriate time. Breach of any Department Policy may result in the same disciplinary action as a breach of policies in this Handbook. If any part of a Department Policy conflicts with a part of these Group policies, the relevant Department Policy will prevail.

II. Some Further Definitions that Apply in this Part B

For clarity, it's useful to set out the defined terms we use for some words and phrases throughout this Part B of the handbook. Some of the other terms used in this Part B **have already been defined in Part A** or are defined in the rest of this Part B.

(a) **Business Group** means any major business line of the Company in Hong Kong, such as Lane Crawford, Joyce or Imaginex.

(b) **Company** means, **for the purpose of this Part B of the handbook**, LCJG Limited and any of its subsidiaries involved in the operation of any of the businesses of the Lane Crawford Joyce Group in Hong Kong (the ***Hong Kong Operations***), including by virtue of being an employer of staff who are involved in the Hong Kong Operations. We may also sometimes refer to the Company by using the words "we" or "our". To avoid doubt on this point, we note that employees of any company that is not covered by this definition will not be covered by these policies.

(c) **employment** means an employee's employment with the Company or any part of it;

(d) **Executive Management** means the Chairman and Chief Executive Officer of LCJG Limited ("**Chairman/CEO**"), the President of any Business Group ("**Presidents**") and any other member of the senior management group of the Company appointed by the Chairman/CEO.

Please note that some defined terms in this Part B are **different from those used in Part A** of the handbook. For example, in this Part B of the handbook the word "**Company**" means all the entities in the Lane Crawford Joyce Group. However, in Part A, "**Company**" is likely to mean only one or a few of those entities. Please check Part A of the handbook for details.

However, in all cases throughout this handbook, the word "Company" will include (i) any successor-in-title to the Company and (ii) any assignee of its rights, whether those rights were granted under the handbook or more broadly.

III. Interpretation and Other Guidance in relation to these Part B Policies

Also for clarity, we note that the interpretation rules explained in Part A of the handbook apply in this Part B. In addition, please see the guidance in Part A concerning employees' and the Company's responsibilities in relation to all the policies in this handbook, the application of 'Applicable Law' to them, the consequences of any breach of the policies and how employees can raise concerns under them.

As with the policies in Part A of the handbook, the policies and provisions in this Part B do not form part of the employment contracts of employees unless we have **expressly noted within a specific policy or provision** that it does have contractual effect. Please note that the policies and provisions in this handbook that do **not** expressly form part of those employment contracts may be varied, replaced or withdrawn from time to time by the Company in its absolute discretion, without notice, to the extent permitted by Applicable Law.

The policies in this Part B of the handbook are provided to Hong Kong staff in both English and Chinese. Please note that if there is any conflict between the two language versions, the English version will prevail.

IV. Departmental Contacts

At various points in this Part B of the handbook, we let staff know that they're welcome to contact one or more Company departments to discuss or raise any concerns relating to the corresponding policies. The contact details for those Departments are as follows:

- **Human Resources**: The employee's usual Human Resources Department representative.
- **Legal**: legal@lcjgroup.com or the employee's usual contact in the Legal Department.
- **Corporate Finance**: CorpFinancePolicies@lcjgroup.com.

GROUP POLICIES

Our Principles: We Maintain a Professional & Respectful Workplace

1. MAINTAINING A HEALTHY AND SAFE WORKPLACE

Reason For This Policy: The Company and employees need to work together to ensure a healthy and safe workplace for all, for the benefit of all.

1.1 Co-operation between Employees and Company

The Company is committed to maintaining safe and healthy working conditions for all staff. It has established the following policies and procedures to help provide those working conditions, but it needs the cooperation of its employees to achieve its goal. It therefore expects all employees to follow these policies and procedures, to act safely and to report unsafe conditions to their Line Manager promptly.

The Company and its employees also need to cooperate in order to comply with environmental, workplace, health and safety laws that apply to us. Employees must follow all notices issued by the Company in this respect, whether in electronic or hard copy form.

1.2 Hygiene, Fire Precautions and First Aid

The Company sets a high standard of hygiene and cleanliness in order to make shopping and working conditions safe and pleasant for customers and employees alike. Employees are expected to keep their work area clean and tidy in order to maintain these hygiene standards.

Employees should familiarise themselves with the locations of emergency exits and fire-fighting equipment within the vicinity of their usual work area. The evacuation map for each of the Company's workplaces is available at staff entrances or from the Administration Department at the One Island South building.

First aid boxes are provided at a number of places in the Company's premises for the convenience of employees. A list of certified first aid caregivers and locations of first aid boxes is also available from the Company's Administration Department in One Island South.

1.3 Workplace Security

Please note: this Workplace Security section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

(a) Staff cards

At the start of each employee's employment, the Company will issue the new employee with either a temporary staff card or a personalised staff card for workplace access and/or identification purposes. If an employee is only given a **temporary** staff card on the start of employment, then they will be given a personalised staff card upon the successful completion of their probation period with the Company. Each employee must keep their temporary or personalised staff card secure, handle it with care and be able to show it at any time during work to prove their identity as a Company staff-member.

Under no circumstances should employees allow any other person to use their staff card. If an employee loses their staff card, they must immediately report the loss to the Company. At its sole discretion, the Company may then require the employee to pay a reasonable fee for a replacement staff card.

(b) Visitors and entrances

Apart from customers visiting our stores, all guests and visitors to Company premises should be escorted by the hosting employee. Please ask guests to log in with the appropriate entry staff at the premises (such as the Receptionist) and ensure that the guest wears the provided visitor badge while in the Company's premises and returns it to the entry staff on departure. Employees should not invite guests to any Company premises outside normal working hours. Meetings at work with families and friends should be confined to the reception/entry area of the relevant workplace.

All entrances of the Company's workplace should be locked after normal working hours. If employees leave the Company's premises after normal working hours, they must secure the door/gate when they leave. Store staff must use only the prescribed staff exits and entrances of the relevant store, unless special arrangements are made in advance or are otherwise reasonably necessary (such as for job duties or health and safety reasons).

(c) Property and staff lockers

The Company's security personnel may inspect the contents of any locker provided to an employee by the Company, or any bag or other personal belongings carried with them, when they leave the Company's premises, as long as the security personnel is accompanied by another person authorised by Company management.

Please do not bring valuables to the workplace. For store staff, no personal items (other than their mobile phone, if used for work purposes) should be brought onto the store floor. While on duty, store employees must not have personal packages delivered to them on the sales floor. Personal packages may, however, be delivered to the authorised Department in stores/boutiques for collection by the individual when he/she is off-duty. The Company reserves the right to check the content of the parcels purported to be employee purchases.

Employees should keep in their lockers (where provided) any property they bring to work, other than their mobile phone if used for work purposes. Employees' lockers should be kept clean and tidy. Employees must not change lockers with another employee, change the locker padlocks or use additional locks on them. On the termination of an employee's employment, the departing employee should clear and clean the relevant locker and return its padlock to the Company. If this is not done by the end of the last day of employment, the Company may remove and dispose of all items remaining in the locker, without notifying or compensative the employee.

The Company will not accept responsibility for property, valuables or cash left in any Company premises. Missing items should be reported to the employee's Line Manager immediately.

1.4 Stock Security

Any loss of merchandise should be reported to the store-in-charge or warehouse management (as applicable) at once. A report of each case should be made by the store-in-charge or warehouse management (as applicable) to the relevant Department Head or Sales/Operations Manager, as appropriate. The Company reserves the right to claim compensation from any employee who it reasonably believes has lost stock.

Store employees who are asked to leave the premises during normal working hours in order to take merchandise for alteration or repair must obtain a stock movement authorisation from their store-in-charge.

1.5 Smoking, Alcohol and Drugs

Please note: this Smoking, Alcohol and Drugs section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

The Company is committed to providing a clean air working environment. As a result, smoking is prohibited in all Company premises, including in offices, stores, warehouses, lift lobbies, toilets, common corridors, staircases and roof terraces.

Employees must not report for work under the influence of alcohol or drugs or consume drugs (except for medication prescribed by a registered medical practitioner) during the course of their work duties. Unless at an internal work function where they are provided employees should not consume alcohol in the course of their work duties. We also recommend that employees not drink alcohol at business functions hosted by Business Partners of other third parties. If, however, refusing an alcoholic drink is problematic at such a function for business courtesy reasons, consumption should be kept to a minimum.

1.6 Reporting an Accident or Injury

Any injury, accident or safety hazard on Company premises must be reported to the Department Manager immediately, who will report the matter in writing to the Human Resources Department, where a full injury record is maintained.

Please do not attempt to repair any Company equipment that is out of order or malfunctioning; instead report it to the Line Manager, who will report it to the Administration Department or I.T. Department (as applicable) to arrange repair.

If a serious accident or injury occurs on Company premises or otherwise to staff in the course of their work duties, the relevant Department head must call an ambulance immediately and then promptly report the matter to the Human Resources Department.

1.7 Employee Wellbeing

Company management cares about our employees' wellbeing and recognises the importance of providing assistance for employees in dealing with personal problems that may adversely affect their job performance. For this reason, we have established the Employee Assistance Programme ("**EAP**"). The EAP is operated for the Company by a designated external professional body that has the resources and professional counselling expertise to help employees in this regard, whether at work or home. All conversations and records involving services provided under the EAP will be treated as confidential and maintained separately from personnel records. There is no cost to staff for their use of the EAP. However, employees will be responsible for any costs they incur in undertaking any recommended treatment. Employees can obtain more information about the EAP from the Human Resources Department or the Company's usual staff communication channels.

The Company also takes pride in offering workplaces that have a positive impact on all aspects of employees' physical, emotional, social, financial and career wellbeing. We emphasise best practices in corporate social responsibility and office ergonomics, and our wellness room at the Company's One Island South premises offers a welcoming physical space to rest and regenerate, as well as hosting various wellbeing initiatives that serve to inform and enrich staff.

To the extent permitted by Applicable Law, employees' participation in such initiatives is undertaken at their own risk.

1.8 Typhoons, Rainstorms and Other Adverse Weather

The Company will follow the procedures set out below during adverse weather events in Hong Kong on working days, including for typhoons, rainstorms and any "extreme conditions" announcement (see explanation below) issued by the Hong Kong government.

(a) Typhoons

Typhoon Signal	Action / Arrangement
No. 1	Office, store and other business operations continue as normal.
No. 3	Office, store and other business operations continue as normal.
No. 8 or above	If the typhoon signal no. 8 ("**T8" signal**) is hoisted **before** office or business hours: • All staff are exempt from reporting to work in their workplace, except for essential staff who are deemed critical to the security or operation of the Company's stores, including (where applicable) the General Services Manager, the Security & Loss Prevention Manager/ Supervisor and the Senior/Security & Loss Prevention Officer responsible for holding the keys to the relevant store. • All employees should work from home, where practicable, in a safe environment. Staff should contact their Line Manager if they have any difficulties with this. If the T8 signal is hoisted **during** office or business hours: • All workplaces will be closed (including the stores) and employees will be permitted to leave for home as soon as practicable, provided that it is safe for them to do so. Essential staff who are required to perform tasks considered critical to the ongoing security or operation of the Company's stores must complete those tasks prior to leaving for home. • Pregnant staff, employees with physical challenges and staff who live on the outlying islands or in in areas where transport services are likely to be suspended will usually be given priority in leaving, where appropriate. • All employees should then work from home, where practicable, in a safe environment. Staff should contact their Line Manager if they have any difficulties with this. For office and warehouse staff only, if the T8 signal is likely to be hoisted during office or business hours of the **following** work day: If the Hong Kong Observatory advises that it is likely that the T8 signal will be issued during office or business hours on the following work day, then at the discretion of their Line Manager, employees may be permitted to work from home and not be required to report to their work location. If the typhoon signal is lowered below T8 **before or during** office or business hours: • All office and warehouse staff are required to report to work at their workplace if the typhoon signal is lowered below T8 by 12:30pm. • Store staff are required to report to work in their store if the typhoon signal is lowered below T8 at a time that is five or more hours before what would have been the end of the individual staff-member's shift that day.

	• Customer Contact Centre staff are required to report to work if the typhoon signal is lowered below T8 at a time that is either (i) on a weekday, five or more hours before what would have been the end of the individual staff-member's shift that day or (ii) on a Saturday, Sunday or public holiday, before 8:00am that day. • However, at the discretion of the relevant head of Department, employees may be permitted to continue working from home and not report for work at their work location that day. • Where staff are not required to report to their work location, they should continue to work from home, where practicable, in a safe environment. *<u>Please note</u>: the schedule for the Company's Shuttle Bus from/to One Island South will be rearranged according to the situations above; the updated schedule will be shared on <u>ijam</u> as warranted.*

(b) Rainstorms

Rainstorm Warning	Action / Arrangement
Amber	Office, store and other business operations continue as normal.
Red	<u>If the warning is issued **before** office or business hours</u>: • Office, store and other business operations continue as normal. <u>If the warning is issued **during** office or business hours</u>: • At the discretion of the relevant Department head or store manager, an early release from work may be given to pregnant staff, staff with physical challenges and staff who live on outlying islands or in in areas where transport services are likely to be suspended. • The relevant Human Resources Department representative should be informed before any early release is given.
Black	<u>If the warning is issued **before** office or business hours</u>: • All staff are exempt from reporting to work in their workplace, except for essential staff who are deemed critical to the security or operation of the Company's stores, including (where applicable) the General Services Manager, the Security & Loss Prevention Manager/ Supervisor and the Senior/Security & Loss Prevention Officer responsible for holding the keys to the relevant store. • All employees should work from home, where practicable, in a safe environment. Staff should contact their Line Manager if they have any difficulties with this. • If any employees are on the way to their workplace when the warning is issued, they should consider the rain, road, slope and/or traffic conditions, and consider whether it is safe to continue their journey to work. <u>If the warning is issued **during** office or business hours</u>: • Staff are encouraged to stay in their workplace for their safety. Office, store and other business operations will continue as normal, as far as it is practicable and safe to do so. • However, if they choose to do so, any staff-member will be permitted to leave their workplace at the discretion of their Department head or store manager.

	If the warning is lowered **before or during** office or business hours: • Office and warehouse staff are required to report to work at their workplace if the black rainstorm warning is lowered to red or amber by 12:30pm. • Store staff are required to report to work in their store if the black rainstorm warning is lowered to red or amber at a time that is five or more hours before what would be the end of the individual staff-member's shift that day. • Customer Contact Centre staff are required to report to work if the black rainstorm warning is lowered to red or amber at a time that is either (i) on a weekday, five or more hours before what would have been the end of the individual staff-member's shift that day or (ii) on a Saturday, Sunday or public holiday, before 8:00am that day. • However, at the discretion of the relevant head of Department, employees may be permitted to continue working from home and not be required to report for work at their work location that day. • Where staff are not required to report to their workplace, they should continue to work from home, where practicable, in a safe environment.

(c) "Extreme conditions" announcements

"Extreme conditions" announcement from HK government	Explanatory note: To heighten residents' alertness about more intense typhoons, and in addition to the issuance of the numbered typhoon signals addressed above, the Hong Kong Observatory labels the most destructive typhoons as 'Super Typhoons'. Where the Observatory **intends to lower Typhoon Signal No. 8 in the wake of such a Super Typhoon**, but that typhoon is expected to continue to cause significant safety concerns in the territory for a prolonged period of time (such as large-scale power outages, major landslides, extensive flooding, serious obstruction of public transport services, etc.) or to seriously affect the ability of residents to resume work, the Government may make a territory-wide announcement that "**extreme conditions**" are expected to apply for at least two hours after the Observatory lowers the T8 signal. If an extreme conditions announcement is made **before or during** office or business hours: • All staff will continue to be exempt from reporting to work in their workplace, except for essential staff who are deemed critical to the security or operation of the Company's stores, including (where applicable) the General Services Manager, the Security & Loss Prevention Manager/ Supervisor and the Senior/Security & Loss Prevention Officer responsible for holding the keys to the relevant store. • All workplaces (including stores) will remain closed. • All employees should work from home, where practicable, in a safe environment. Staff should contact their Line Manager if they have any difficulties with this. If the extreme conditions announcement is cancelled **before or during** office or business hours: • if the extreme conditions announcement is cancelled by 12:30pm, office staff are required to report to work at their workplace.

	• Store staff are required to report to work in their store if the extreme conditions announcement is cancelled at a time that is **five or more hours before** what would be the end of the individual staff-member's shift that day. • Customer Contact Centre staff are required to report to work if the extreme conditions announcement is cancelled at a time that is either (i) on a weekday, **five or more hours before** what would have been the end of the individual staff-member's shift that day or (ii) on a Saturday, Sunday or public holiday, **before 8:00am** that day. • However, at the discretion of the relevant head of Department, employees may be permitted to continue working from home and not report for work at their work location at all during that day. • Where staff are not required to report to their work location, they should continue to work from home, where practicable, in a safe environment.

(d) General guidance:

- Essential staff who are required to report for work at their workplace during adverse weather conditions should carefully plan in advance a safe route and appropriate transport for commuting to their workplace. They should consult their Line Manager or store manager in the event of difficulties in travelling to their workplace.

- If, during office or business hours, a typhoon signal No. 8 or above is lowered to below T8, or an extreme conditions announcement is cancelled or a black rainstorm warning is lowered or cancelled, and staff are unable to report for work at their workplace within **two hours** after that lowering or cancellation, they should obtain the approval of their Line Manager to stay at home.

- Store employees who are working in a shopping mall or department store should follow the guidelines set by the relevant shopping mall or department store.

- Employees who fail to report for work at their workplace without a valid reason may be subject to disciplinary action. However, the safety of employees during adverse weather will be the Company's prime consideration.

2. PROFESSIONALISM, FAIRNESS AND RESPECT FOR OTHERS

Reason For This Policy: The Company is committed to maintaining a work environment where each employee acts professionally, is treated fairly and with respect, and where every employee is given an equal chance to succeed.

2.1 Employee Code of Conduct

Please note: this Code of Conduct section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

Employees are required to observe the Company's rules, regulations and policies, including this Code of Conduct in order to maintain the integrity and effectiveness of the Company. If any employee has any doubts as to the correct course of action in respect of any of the matters below or in other policies of this handbook, they should consult their Line Manager, Department head or the Human Resources Department.

(a) Ethical behaviour

The Company regards integrity, honesty and fair play as valuable assets for conducting business, which are of paramount importance to the long-term development and success of the Company. Employees must uphold the Company's ethical reputation by practising fairness and integrity in our work. Please also see the Fair Business Practices policy in this Part B of the handbook.

(b) Professionalism and respect

In the course of their work for the Company, employees must always behave in a responsible and professional manner and treat with courtesy and respect our colleagues, customers, Business Partners and any other third party with whom they come into contact.

(c) Punctuality

Please note: this Punctuality section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

Punctual attendance at the workplace is a standard expectation of all Company employees, as it contributes to the efficient operation of the Company and a smooth workflow for colleagues. Employees must report for work on time, in accordance with their agreed working hours. The Company will consider persistent lateness or numerous early departures by employees to be serious misconduct and, as such, may take disciplinary action against relevant employees as a result.

(d) Extra-curricular activities at work

Employees must not sell tickets, post notices or take collections or donations on Company premises without the prior consent of the Company.

(e) Loans

Employees must not borrow money from other employees. If any employee has genuine financial problems, they should discuss the issue with their Line Manager, Department head or the Human Resources Department.

(f) Dress code

If the Company provides an employee with a uniform for work purposes, the employee must wear that uniform (including any name tag, if provided) while at work for the Company, but not outside of it. The uniform must be kept clean and in good condition. If any part of the uniform is lost, the employee must immediately report that loss to the Company. At its sole discretion, the Company may then require the employee to pay a reasonable replacement fee.

If employees are not required to wear a uniform for their role with the Company, they are still expected to present a clean, professional appearance, in attire that is appropriate for their job duties. Please respect your workplace and your colleagues, and do not wear clothing that is stained, torn or overly revealing.

2.2 Equal Employment Opportunities

The Company believes in equal employment opportunities and in creating, managing and valuing diversity in our workforce. As a result, we will not make employment-related decisions based on a person's gender, race, national origin, ethnicity, age, sexual orientation, family status, pregnancy, religion, physical appearance, name, physical or mental disability or any other characteristic that is protected by Applicable Law.

2.3 Protection against Discrimination, Harassment, Vilification and Victimisation

The Company is also committed to providing a workplace that is professional and respectful, free from discrimination, harassment, vilification and victimisation.

We will not tolerate in our workplace **any** form of discrimination, sexual or other harassment, vilification or victimisation, whether committed against any colleague, Related Party or any other person protected by Applicable Law.

(a) Definitions

Discrimination includes both direct discrimination and indirect discrimination.

- *Direct* discrimination may vary under local law but, broadly, it means treating a person less favourably than another person, in comparable situations, because of that person's protected attributes or circumstances, such as gender, sexual orientation, gender identity, age, political or religious views, marital or family status, pregnancy, maternity or paternity, race, ethnic or country of origin, nationality, religion, physical appearance, name, place of residence, medical conditions or disability, as well as any other characteristics that are protected under Applicable Law ("**Personal Attributes or Circumstances"**).

- *Indirect* discrimination broadly consists of applying the same treatment as between persons with different Personal Attributes or Circumstances which is discriminatory in its effect.

Harassment broadly means:

- unwelcome conduct towards a person in relation to that person's Personal Attributes or Circumstances (e.g. conduct based on their race, physical appearance, sexual orientation, etc., such as in circumstances where a reasonable person would have anticipated that the harassed person would be offended, humiliated or intimidated; or

- unwelcome conduct with the purpose or effect of impacting the harassed person's dignity, health or working conditions.

It includes offensive jokes, slurs or name calling, threats, bullying (whether in person or online), mockery, insults or put-downs, offensive objects or pictures, or interference with work performance. It can be physical, verbal, sexual or emotional harassment.

Vilification broadly means any activity in public to incite hatred towards, serious contempt for or severe ridicule of a person on the grounds of that person's Personal Attributes or Circumstances. "Activity in public" includes any form of communication, any conduct observable by the public and the distribution or dissemination of any matter to the public.

Victimisation broadly means retaliating against someone who in good faith makes or helps to make a complaint about harassment and/or discrimination, cooperates with an investigation into such a complaint, or files a claim about harassment and/or discrimination with a court or local labour authority. Victimisation may also include retaliation against so-called "whistleblowers" – please see the Company's Policy on **Whistleblowing** further below.

Workplace for this purpose includes **<u>any</u> work-related setting**, whether inside or outside an employee's usual place of work, including on business trips, at business meetings and during business-related social events.

The Company will also not tolerate any retaliation against an individual who has reported or complained about any of the above behaviours or who has co-operated with an investigation into such a complaint.

(b) Complaints of Discrimination, Harassment, Vilification or Victimisation

If any employee believes that they have been subjected to any form of discrimination, harassment, vilification or victimisation in the course of their employment, the employee has the right to file a complaint with the Human Resources Department or a member of the Company's Executive Management (please see the definition of Executive Management in the Introduction to this Part B of the handbook), asking that the complaint be investigated by way of the Company's grievance procedure. The Company's formal grievance procedure is also set out in this Part B of the handbook.

No employee will be penalised for making such a complaint or raising a grievance in good faith. The Company will endeavour to keep such complaints confidential, as far as is practicable in the context of the specific investigation.

2.4 Disclosure of Criminal Convictions

Please note: this Disclosure of Criminal Convictions section is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

The Company requires most job candidates to disclose to it whether they have any criminal convictions as at the date that they apply for a role with the Company. If any employees are convicted of a criminal offence **after** the start of their employment with the Company, they must promptly disclose that conviction to the head of their Human Resources Department.

If a staff-member fails to so disclose a criminal conviction promptly, the Company may terminate that staff-member's employment with immediate effect at any time, and with no obligation to make any payment or other compensation to the staff-member.

3. FORMAL GRIEVANCE PROCEDURE

Reason For This Policy: The Company has established this formal grievance procedure to encourage a thorough, prompt and satisfactory resolution to issues or concerns raised by any employee about aspects of their work (a "**grievance**"), including their work environment, working relationships, health and safety matters and the application of policies to staff.

We believe that formal grievance procedures can promote a healthy and informed grievance culture within a company, allowing the resolution of issues in a transparent and speedy manner and protecting important working relationships before a problem escalates further. It is important to state that no employee will be penalised for making a grievance claim in good faith. All such employees will be listened to and we will endeavour to keep employees' claims confidential, as far as is practicable in the context of the specific investigation.

We ask all employees to be aware that a work-related grievance can be raised by an employee in respect of an issue that has occurred **outside the Company's premises**, provided that the incident took place during activities related to an employee's employment with the Company, such as at a Company event or a client or off-site meeting.

3.1 Principles

The Company strongly encourages staff to **promptly** raise grievances via this grievance procedure.

Once the Company receives a grievance claim, it will aim to investigate the allegation within the shortest amount of time practicable and to achieve a fair and just outcome to all concerned.

To the extent practicable in the context of the specific investigation, the Company will endeavour to keep grievance investigations confidential. At any stage during a grievance procedure, an employee should feel free to contact the head of their Human Resources Department if assistance or advice on the procedure is needed.

3.2 Grievance Procedure

If possible – and if the employee believes it is both constructive and **safe** to do so – an employee may first attempt to **informally** resolve an issue that arises in the work context. For example, employees who are the target of unwanted conduct may try to express clearly to the person engaging in the unwanted conduct that the behaviour in question is not welcome, that it offends them or makes them uncomfortable and that it interferes with their work and/or well-being. They may also inform the Human Resources Department about their conversation with that person.

If the unwelcome conduct or other issue continues or if the employee believes it is not appropriate to try to resolve the problem informally, the employee should consider making a grievance claim to the Company. We have described below how employees can do this and what an employee can expect during the grievance process.

(a) Beginning a grievance claim – please contact HR

To begin a grievance claim, employees are encouraged to contact their Human Resources Department as soon as possible about the incident(s) central to the grievance, whether by phone, email or in person. The employee should try to provide as much detail as they can at this stage, including (where applicable):

- when and where the incident(s) took place;
- who committed the incident(s);
- who else was present at the time; and
- what the effects of the incident(s) have been on the employee.

If the employee knows of any physical evidence of the incident (such as the possibility of a CCTV recording), please also let the Human Resources Department know this.

(b) HR meets with the employee to discuss the grievance and process

Within one week of the employee's initial contact with the Human Resources Department about the grievance, an appropriate Human Resources Department representative ("**HR Representative**") will hold an in-depth meeting with the employee to discuss with them the full details of the grievance and any questions or other topics raised by it. The employee should feel free during the meeting to provide additional details and to ask the HR Representative any questions they have about the grievance process.

At that meeting the HR Representative will also let the employee know how long the investigation of their grievance will take. In most situations, the Company expects that the HR Representative will take no longer than two weeks from that point to investigate the grievance, make a decision on it and, where needed, any action to be taken in respect of it ("**Decision**"), and meet again with the employee to discuss the Decision.

(c) HR investigates the grievance

After the grievance meeting with the employee, the HR Representative will promptly investigate the grievance and try to decide on and resolve it in a fair and just way. To do this, the HR Representative will work to:

- fully understand the details of the grievance and plan out the investigation process appropriately;
- identify relevant witnesses, other affected parties and other evidence;
- follow up with the employee about questions or evidential conflicts that may arise during the investigation, so that the employee may give their view on them;
- investigate the grievance thoroughly and objectively, as well as consistently with the above principles and other similar investigations by the Company, in order to reach a fair and just finding about the grievance; and
- keep clear and confidential written records of all investigation details and the decision on it.

Where necessary, an HR Representative investigating a grievance may consult with the Legal Department about it, the investigation process and/or the proposed Decision.

(d) HR discusses decision with employee

By the end of the above three-week period, the HR representative will meet with the employee to advise them of the Decision and to fully discuss it with the employee in detail.

This meeting will take place in person if the employee and HR Representative) are in the same location, or via a video platform if they are in different locations. The employee can request that the meeting take place in a different way, such as by phone.

Actions that may be proposed by the HR Representative as part of a Decision that **upholds** a grievance claim include:

- imposing appropriate disciplinary action on any offending party who is an employee and/or considering changes to the working environment of an affected employee;
- if any individual from a third party is an offending party, reporting the complaint to the employer of the third party with a request that the conduct be investigated and appropriate action be undertaken; and
- in either case, considering and then fully discussing with the reporting employee how they can best move forward from the claim and whether any further reporting should occur, such as to the relevant authorities.

(e) Appeal process - Appeal statement to Company management

If the employee is not satisfied with the Decision or any proposed actions, the employee should instead submit a formal statement in writing to the head of the Human Resources Department or the Legal Department.

To help those executives investigate the appeal statement quickly and properly, please again provide the fullest information possible about the grievance, as well as the employee's reasons for their dissatisfaction with any prior Decision. The executives will then undertake their own investigation in a prompt and fair manner, as detailed further above. They will meet with the employee within a maximum of four weeks to advise of their Decision.

If the nature of the grievance is such that the employee believes they cannot discuss their grievance claim with the Human Resources Department, the employee should instead submit a formal grievance statement in writing to the Legal Department, who will follow the same process and timeline as set out further above.

The Company notes that employees may also choose to lodge a complaint with, or consult for guidance, the Hong Kong government's Labour Department about any work-related grievance at any time.

3.3 Anonymous Grievance Claims

While employees may report grievances anonymously, the Company strongly recommends that any grievance claim be submitted in the reporting employee's name, due to the fact that it is usually very difficult for the Company to investigate an anonymous grievance claim as well as it would like. We understand that grievance complaints are very important and, often, very personal. Accordingly, we want to give our investigation into any grievance the best chance of success. However, when the Company receives an anonymous grievance claim, we are often unable to take some key investigative steps, such as discussing follow-up questions, clarifications or evidence with the complainant, which makes it difficult to assess the claim appropriately and with the full context of the relevant situation. Employees have the right to be safe at work and to perform their roles without inappropriate conduct taking place around them, but the Company also owes rights to other staff or third parties to fully investigate grievance claims against them and not merely take a complainant at their word.

Anonymous grievance claims can also make it challenging for the person investigating the grievance to know whether the actions they intend to propose to help resolve the claim will actually be sufficient, because they do not know who those actions are principally intended to help. In addition, anonymous grievance claims can result in the complainant not having a sufficient voice in the investigation, which can undermine the usefulness of the grievance process. Employees should therefore be aware that the Company's ability to investigate and/or act upon an anonymous grievance claim may be more limited than the employee would wish.

For all these reasons the Company greatly prefers that, during the reporting process, the complainant employee(s) make themselves known to the investigating person or to the Human Resources Department, the Legal Department or any executive mentioned in this grievance policy. Those executives would like to reiterate that any employee making a grievance claim in good faith will not be subject to any retaliation by the Company and that the Company will endeavour to keep such claims confidential, as far as practicable in the context of the specific investigation.

4. POLITICAL NEUTRALITY

Reason For This Policy: Our business is about bringing joy to our customers without opinion, judgment or agenda; employees' political views have no place in the business.

4.1 Expressing Political Views in the Workplace

The Company believes that everyone has the right to express their political views in their personal lives and in accordance with Applicable Law. However, in our role as representatives of the Company, we take a neutral stand at all times on all issues related to politics.

While at work or when otherwise performing any activity in which they could be seen to be representing the Company, employees must:

- respect the Company's policy of neutrality in relation to political matters, regardless of whether the employee is conversing with colleagues, customers, Business Partners or other third parties, or whether such communications take place in person, by email or messaging, on social media or by any other communication method;

- understand that any political view by them is only acceptable in the employee's personal capacity and that they must make clear, at the time the view is expressed, that the view represents only the employee's personal view; and

- ensure that any personal view they express is respectful of Applicable Law, the Company's policies and the best interests and good standing of the Company.

4.2 Time Away from the Workplace for Political Activities

The Company acknowledges that employees may wish to attend different political activities outside of the workplace from time to time. If employees wish to participate in political activities that require time away from work, this time will be treated as an absence from work for a personal activity. Accordingly, for such an absence, employees must go through the normal process of applying for leave or another approved absence in accordance with this handbook, Applicable Law. Any unapproved absence will also be dealt with in accordance with the relevant provisions of those resources.

Our Principles: We Respect Confidentiality, Intellectual Property and Personal Data Privacy

5. PROTECTION OF COMPANY'S CONFIDENTIAL INFORMATION

Please note: this Protection Of Company's Confidential Information policy is contractual in its effect and applies **in addition to** any confidentiality obligations under an employee's employment contract or any separate confidentiality agreement.

Reason For This Policy: Confidential and other proprietary information is an important resource in the Company's business. It often results from significant time and work by the Company. Disclosure of this information is likely to undermine and significantly damage the Company's business.

5.1 What is Confidential Information?

One of the important responsibilities of being an employee of the Company is to protect the confidential information relating to the Company or its operations and all other proprietary information of the Company ("**Confidential Information**"). Confidential Information is not usually limited by its form or the way in which it has been delivered or received. It therefore includes both

physical and digital material and information that is transmissible in hard copy, electronically or even verbally.

Whether any information is deemed to be Confidential Information of the Company is ultimately a question of fact, but it is reasonable for employees to assume that:

- information belonging to or about the Company, its operations or its business relationships will be deemed confidential if that information is not readily available to persons not connected with the Company; and

- as such, that information will not be deemed information which forms part of the employee's "skill and knowledge" (i.e. it will not form part of an employee's so-called "stock in trade").

Examples of Confidential Information include: the Company's strategic or business plans or current or proposed deals; its past, current or future financial results; its lists or details of its customers or Business Partners; employment-related information about its staff; and information concerning the Company's policies and business processes.

5.2 Employee Obligations in relation to Confidential Information

- **Do not disclose Confidential Information:** Employees must not disclose, exploit or use, whether directly or indirectly, for any reason other than the legitimate business-related purpose for which the employee accessed or received the information ("**Legitimate Purpose**"), any Confidential Information that the employee has accessed or received as a result of their employment. They also must not copy, save, print or by any other means reproduce Confidential Information, whether stored in electronic or hard-copy forms, onto any electronic or hard copy form or devices, other than for a Legitimate Purpose unless they have the prior written authorisation of the Company.

- **Keep all Confidential Information secure:** Employees must use their best efforts to keep safe all Confidential Information in their possession or control, whether electronically or in hard copy, and must comply with any additional requirements placed on any specific Confidential Information or category of Confidential Information.

- **Do not use others' confidential information inappropriately:** Employees must not use confidential information of a third party through unlawful or inappropriate means, such as the breach of a non-disclosure agreement or a former employment agreement.

5.3 Duration of Confidentiality Obligations and Consequences of Breach

The Confidential Information obligations in this policy **apply during and after** an employee's employment with the Company.

In addition to its other rights and remedies, the Company reserves the right to take appropriate legal action against any employee if they breach any of these Confidential Information obligations, whether to recover any Confidential Information, to claim damages arising from the breach in accordance with Applicable Law or to obtain any other permitted remedy.

Employees are also cautioned that unauthorised disclosures of **personal information** about Company staff, Related Parties or other individuals may constitute a separate legal offence under local data protection laws. Please see the Company's Protection of Personal Data policy in this handbook.

6. PROTECTION OF INTELLECTUAL PROPERTY RIGHTS

Please note: this Protection Of Intellectual Property Rights policy is contractual in its effect and applies **in addition to** any other intellectual property obligations under an employee's employment contract or any separate agreement. This policy also acts as a Personal Information Collection Statement for the purposes of the Ordinance (defined below)

Reason For This Policy: The Company's business relies on intellectual property such as designs, brand names, illustrations and other works of creative effort. It respects the intellectual property of others and expects its employees to do the same.

6.1 What are Intellectual Property Rights?

"**Intellectual Property Rights**" means patents, Inventions, copyright, trademarks, trade names, domain names, goodwill, design rights, database rights, confidential information, trade secrets, moral rights, proprietary rights and any other intellectual property rights (whether registered or unregistered) and including all applications, renewals or extensions of such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world.

6.2 Protection of Intellectual Property Rights belonging to the Company or Third Parties

Employees must respect all Intellectual Property Rights and comply with all applicable intellectual property laws when dealing with copyrighted material and other intellectual property owned by the Company or others.

For example, unless it is expressly stated to be available for use by the general public, employees should not use for their Company work any other person's designs, work product or other intellectual property, including any that is posted on social media or otherwise on the internet, without the consent of the owner of that intellectual property. Consent may be obtained through, for example, a creative commons licence or another form of written consent from the owner or their agent. Employees also should not use the Company's Electronic Systems (defined further below in this handbook) to download copyrighted material from such locations as peer-to-peer networks without the consent of the copyright owner.

6.3 Intellectual Property Rights in Company Innovations

It is possible that Employees may create inventions, ideas, discoveries, developments, improvements or innovations, processes, formulas, models or prototypes, whether or not patentable or capable of registration, and whether or not recorded in any medium ("**Inventions**") and works of authorship, copyright works, computer programs, databases, designs, trade secrets or other work products of any nature ("**Works**"), collectively known as "**Innovations**").

Employees must promptly and fully disclose to the Company any Innovations and intellectual Property Rights in them that they devise or create, whether alone or with others, in whole or in part, and which:

- was devised or created in the course of the employee's employment with the Company; and/or
- relates in any way to the present or future business of the Company; and/or
- uses or has used the resources of the Company in its conception or creation; and/or
- relates to, and is capable of being used in, those aspects of the business of the Company that are connected to the relevant employee's employment,

(known as "**Company Innovations**" and "**Company Intellectual Property Rights**" respectively).

All rights, title and interest in and to the Works will vest in the Company and be the absolute property of the Company (the "**Company Rights**").

Employees must take all necessary, lawful steps as the Company may require in order to ensure they comply with their obligations under this Intellectual Property Rights policy, including (at the Company's cost) giving all necessary assistance to the Company to vest such Company Rights in the relevant entity of the Company or its directed nominee, to register them in the name of the relevant entity of the Company and to protect and maintain them.

This may require employees to take actions and execute documents that the Company believes to be reasonably necessary to vest all the Company Rights (to the extent permitted by Applicable Law) in the relevant entity of the Company or its directed nominee and to secure all appropriate forms of protection, defence and enforcement of the Company Rights. No employee may do anything (whether by act or omission) during the employee's employment or at any time after but that might prejudice the Company Rights under this section.

In addition, except to the extent prohibited by or ineffective in Applicable Law, each employee:

- assigns by way of present and future assignment to the relevant entity of the Company or its directed nominee, with full title guarantee, all such Company Rights to which that employee may, at any time after the date of the relevant employment contract, be entitled by virtue of any Applicable Law in any part of the world, for the full period of the protection of such Company Rights including all renewals, reversions and extensions; and

- agrees to irrevocably and unconditionally waive all present and future "moral rights" in respect of any Company Innovations embodying Company Rights that arise under the Copyright Ordinance in Hong Kong or any equivalent, replacement or other Applicable Law and other similar rights arising under the laws of any jurisdiction.

6.4 Survivability of Rights and Obligations relating to Intellectual Property

The rights and obligations under this Intellectual Property Rights policy will continue in full force and effect even after the termination of an employee's employment (in respect of Company Innovations made by that employee during the employment) and will be binding on that employee's legal successors.

7. PROTECTION OF PERSONAL DATA PRIVACY

Reason For This Policy: In the course of its business, the Company collects data from many organisations and individuals, including from employees and customers. Some of this data is deemed to be "Personal Data" by Applicable Law and is protected by those laws. The Company is committed to transparency in its collection and use of Personal Data and to ensuring that its data privacy practices – and those of its staff – comply with Applicable Law.

This Personal Data Privacy policy deals with:

(a) the obligations imposed by data privacy laws generally;

(b) the data privacy obligations **owed by the Company to its employees**; and

(c) in brief, **the data privacy obligations owed by the Company and its employees to its retail customers** ("**Customers**"), whether in-store or online, and **other third parties** whose Personal Data is collected by the Company.

7.1 Overview of Personal Data Obligations in Hong Kong

(a) "Personal Data"

In Hong Kong, the collection, use and other dealings with the "personal data" of people is mainly regulated the Personal Data (Privacy) Ordinance, which is an "Applicable Law" for the purposes of this handbook.

Under Applicable Law, "**Personal Data**" in relation to a person includes such things as their name, address, telephone number, Hong Kong Identity Card and passport numbers, image, voice and **any other data from which that person can be identified**.

For example:

- in respect of employees, Personal Data also includes their employment history with the Company; and
- in respect of Customers, it includes credit or debit card numbers and purchase history records.

(b) Categories of people to whom data privacy obligations are owed

The Company owes legal obligations to **employees** in respect of the Personal Data it collects about them. It also owes such obligations to people **outside** the Company from whom the Company collects Personal Data, including Customers and other third-party individuals. For example, it owes these obligations to any employee's next-of-kin whose details have been provided to the Company for emergency contact purposes.

By virtue of the employment by the Company, **employees also owe legal obligations to these Customers** in respect of the Customers' Personal Data. Those obligations can be found in the external-facing Privacy Policy for each of the Company's Business Groups (the "**External Privacy Policies**") and are also summarised further below. Each Business Group's External Privacy Policy is posted on its respective website, such as www.LaneCrawford.com.

If an employee has any involvement with any Customer's, employee's or third party's Personal Data as part of their employment, **they must ensure that they are familiar with their obligations under the relevant privacy policies** and that they carry out those obligations fully and in good faith. If any employees cannot find the relevant External Privacy Policy on their Business Group's website, please contact the Legal Department (legal@lcjgroup.com).

The Company's privacy policy in respect of **employees'** Personal Data is further below.

(c) Data privacy obligations generally

Regardless of whether the Personal Data is collected from employees or Customers, the Company is only permitted to collect Personal Data for lawful purposes that are directly related to a function or activity of the Company. Applicable Law requires that the Company's collection of Personal Data for those purposes must not be excessive.

The Company must protect the collected Personal Data against unauthorised disclosure and must allow employees and Customers the opportunity to access their own Personal Data and, **if inaccurate, have it corrected** by the Company.

The Company will take reasonable steps to ensure that employees and Customers are aware of certain other information related to their Personal Data collected by the Company, including:

- the purposes for which the Company has collected their Personal Data;
- the types of organisations to which the Company may disclose their Personal Data; and
- any law that requires particular Personal Data to be collected from a person, and whether it is mandatory under that law for that person to provide the Personal Data and the main consequences for the person if the Personal Data is not provided.

The Company will also take reasonable steps to:

- ensure that the Personal Data it collects, uses or discloses is accurate, complete and up to date;
- not keep Personal Data longer than is necessary for the fulfilment of the purpose(s) for which the data is or will be used; and
- take reasonable steps to protect the Personal Data it holds from misuse, loss, unauthorised access, modification or disclosure.

Each employee agrees to take such actions and execute such documents as are reasonably required by the Company to (i) give full effect to the rights granted to the Company in this policy and (ii) enable the Company to comply with its obligations under this policy or the External Privacy Policy.

(d) Data Privacy Officers

For Hong Kong law purposes, the Company has appointed (i) its Human Resources Department to act as its Data Privacy Officer in respect of all employee Personal Data and (ii) its Legal Department to act as its Hong Kong Data Privacy Officer in respect of all other data protection matters. Each Hong Kong Data Privacy Officer oversees the Company's compliance with its data protection policies and Applicable Law. They handle employees', Customers' and other third parties' queries about their Personal Data that is collected and/or held by the Company, including any requests for access to their stored Personal Data and any complaints of inaccuracies in or misuse of that data.

Employees should always feel free to contact the Human Resources Department to discuss any privacy questions or concerns they may have about their Personal Data held by the Company. They should also feel free to contact the Legal Department (legal@lcjgroup.com) about any privacy questions or concerns they may otherwise have.

7.2 Company's Collection and Use of Employees' Personal Data

In this section of the policy, we set out specifically the legal obligations and rights concerning the **Company's collection and use of the Personal Data of employees**.

(a) Purposes of collection of employees' Personal Data

The Company may collect employees' Personal Data from both employees themselves and third parties in connection with each employee's employment, in accordance with each employee's contract of employment with the Company and this policy. The Company may use employees' Personal Data (whether in an individual or aggregated manner, and in both Hong Kong and non-Hong Kong locations) for employment-related or business development-related purposes ("the "**Collection Purposes**").

The Collection Purposes include:

- Administering salaries and benefits;
- Considering employees for the purposes of promotions, performance reviews, training, secondment, transfer, career development or manpower planning purposes;
- Facilitating communications between the Company and the employees or between employees themselves;
- Providing employment references;
- Ensuring and monitoring a healthy and safe workplace for staff;
- Observing in-store and customer service employees' performance in order for the Company to understand the quality and level of service provided to our Customers, so as to improve our customer experience. In-store employees will be selected randomly in these unannounced and anonymous observation exercises, which will be done through third party service providers who will commit to Personal Data protections. All calls and messages to the Company's customer service contact points are or may be monitored;
- Administering and reviewing the Company's human resources policies and practices, including staff training purposes;
- Effecting the Company's business and operations, including assessing the Company's business structure, planning for business development and promoting and/or marketing the Company or its goods or services;
- Activities required under or in compliance with law; and
- Other purposes that are directly related to the Collection Purposes.

(b) Employees' provision of third parties' provision of Personal Data

From time to time, employees may also be required to provide the Company with various third parties' Personal Data (for instance, in relation to reference checks or an employee's family members for benefits-related purposes). All employees agree that, before they provide a third party's Personal Data to the Company, they will obtain that third party's consent to the employee's provision of that data to the Company.

The Company will handle all such third party data in accordance with this policy.

(c) Use of likeness

For the avoidance of doubt, by accepting this handbook and in consideration for their employment with the Company, all employees:

- permit the Company or any of its representatives, agents or contractors to photograph, film and/or record them ("Production") for any Collection Purpose;
- to the best of their ability, agree to adhere to the timetable and other reasonable requirements agreed upon prior to the beginning of their involvement in any Production;
- grant the Company the irrevocable but non-exclusive, royalty-free, perpetual, transferable, sub-licensable, worldwide right to use, solely during its employment-related data retention period, in all forms or manner and via any means or media as the Company sees

fit, the relevant employee's voice, image, likeness, professional name and biography ("**Specified Characteristics**") for any Collection Purpose, including:

- reproducing, editing or creating derivative work from the Specified Characteristics;
- incorporating in whole or in part the Specified Characteristics in any materials; and/ or
- publishing, exhibiting, distributing, or sublicensing any materials containing the Specified Characteristics produced by or on behalf of the Company ("**Company Materials**"), including but not limited to, any content posted on social media showing the employee wearing or using goods owned or offered by the Company or any materials created from any Production,

for a Collection Purpose;

- irrevocably waive all moral rights that they may have in any Production;
- irrevocably waive all rights to inspect or approve the Specified Characteristics in any Company Materials for any Collection Purpose;
- agree not to bring any claim or action of any kind against the Company in connection with the use of the Specified Characteristics as permitted above, provided such use is in compliance with Applicable Law; and
- do such acts and execute such documents as are reasonably required and requested by the Company to give full effect to the rights granted to the Company by this policy.

The Company has no obligation to use the Specified Characteristics. It will not use the Specific Characteristics beyond its specified retention period for such information.

During the course of their employment, Employees also agree not to permit, without the Company's prior written consent, the use of their Specified Characteristics to promote or advertise any product, service or organisation that is not affiliated with the Company.

(d) Retention and security of employees' Personal Data

The Company will retain employees' Personal Data only for as long as is reasonably necessary to fulfil the Collection Purposes, and in any case for no longer than seven years after the termination of the relevant employee's employment (unless as otherwise consented to by the employee or as required by Applicable Law). However, the Company may retain an employee's Personal Data for longer than that seven-year period for the purpose of the potential or actual employment of the employee by another part of the Company, including by another of the Company's Business Groups.

All Personal Data of employees that is collected and held by the Company will be treated in strict confidence and in accordance with Applicable Law, and will be protected with all reasonable security measures. The Company discourages staff from saving their Personal Data on the Company's electronic systems, including its email system. If employees have stored Personal Data within the Company's email system, this Personal Data will be held both locally and on the Cloud-based platform(s) on which the Company's email system is hosted. The Company enters into contracts with its Cloud service providers which include stringent data protection measures.

The Company will not use, transfer or disclose employees' Personal Data except for the purposes described in this policy.

(e) Transfer or disclosure of employees' Personal Data to third parties

The Company may transfer or disclose employees' Personal Data to third parties from time to time in connection with the Collection Purposes set out in this policy, provided that those third parties are (where reasonably practicable) subject to privacy obligations materially equivalent to those set out in this policy.

The third parties to which the Company may transfer or disclose employees' Personal Data include:

- Agents, contractors, consultants and third-party service providers (whether in Hong Kong or elsewhere) of the Company in connection with the operations of the Company, e.g. external auditors, medical practitioners, benefits administrators and insurance companies;
- Relevant Government authorities as required by law, e.g. the Hong Kong Police, the Inland Revenue Department and the Labour Department of Hong Kong;
- Any company controlled by or under common control with the Company; and
- Any other persons, firms, authorities or companies, where the transfer or disclosure is (i) prior approved by the relevant employee, or (ii) required by law or court order.

The Company may also transfer employees' Personal Data to third party service providers in order to effect the business operations of the Company.

(f) Employees' access to their Personal Data

Employees must ensure that they notify the Company when their data held by the Company changes – e.g. due to a change of address, telephone number, dependants' details, etc.

Any employee may request the Company to:

- advise the employee of the extent of Personal Data that the Company holds on that employee;
- grant that employee access to a copy of that Personal Data (if any); and
- request the Company to correct any inaccuracies (if any) in the Personal Data held.

The Company may charge the employee a reasonable handling fee to effect any such request. However, the Company will waive this fee if the access is necessary to make a genuine and reasonable correction to that data. All such requests should be addressed to the Human Resources Department.

7.3 Company's Collection and Use of Customers' Personal Data

In this section of the policy, we summarise the **obligations of employees** involved in the Company's collection and use of the Personal Data of Customers ("**Customer Data**"). Please note that **this is a summary only**. Full details are in the protocols that are noted below.

The Company has adopted specific **data collection, access, use and protection protocols** to safeguard Customer Data in accordance with Applicable Law. Those protocols are contained in:

(i) this policy;

(ii) the External Privacy Policy relevant to each Business Group and posted on their websites; and;

(iii) the training and procedures communicated to employees who handle Customer Data in the course of their employment. All these protocols are updated from time to time, as necessary.

If an employee's role requires them to be involved in any handling of Customers Data, whether collection, storage, access or any other use, such employees **must** familiarise themselves with all these protocols and comply with the Company's obligations in respect of Customer Data that are set out in them.

(a) Collection of Customer Data

As with the Company's collection of employee Personal Data, the Company may only collect Customer Data for lawful purposes that are directly related to a function or activity of the Company, and that collection must not be excessive for the relevant purpose. Those purposes may include:

- providing the Customer with products or services they have requested from the Company;
- improving our services to Customers, responding to Customer preferences and conducting marketing activities;
- supplying Customers with direct marketing communications in relation to our products, services, events and promotions, **but only if** we have those Customers' express prior consent in respect of direct marketing communications;
- monitoring and analysing consumer trends, usage, browsing and shopping behaviour at our stores and websites;
- sharing **strictly relevant** Customer Data with third party service providers within or outside of Hong Kong who will process Customer Data on our behalf for the purposes identified above or in our websites' privacy policies, such as courier service providers, email and mobile message service providers, data storage and cloud service providers, online advertising platforms (with express consent) and data analytics service providers; and
- any other purposes permitted or required by applicable personal data/privacy laws and regulations, as long as we have obtained, where applicable, the necessary prior written consent of the relevant Customers and all required approvals from the relevant authorities.

Employees who work with Customers will be required to provide a Company-supplied notice (a "**Personal Data collection statement**") to each Customer as soon as reasonably practical after that customer provides the Company with Personal Data. The notice will contain information about the Company's protocols in respect of the use and protection of Customer Data and will include a link to the relevant division's External Privacy Policy.

Please note: the Company cannot compulsorily require Customers to provide a copy of, or the number of, the Customer's Hong Kong identity card ("**ID Card**"). As a result, employees must **not** request the number of a Customer's ID Card, except where:

- the use or collection of the ID Card number by the Company is necessary to identify the Customer Data for the Customer's benefit or to prevent detriment to others; or

- where the collection of the ID Card number is required by Applicable Law, in which case the Legal Department **must** be consulted **prior** to the employee collecting that number. The Legal Department is available at legal@lcjgroup.com or employees can directly consult their usual contact in the Legal Department.

Employees should never keep a copy of a Customer's ID Card.

Before asking a Customer to provide an ID Card number, the employee must consider whether there are any less privacy-intrusive alternatives to the collection of the number (e.g. by instead collecting the Customer's mobile telephone number, driving licence number, etc.) and then give the Customer the option of providing one of those alternatives instead.

Access to those ID Card numbers that have been lawfully collected by the Company is only permitted for those employees who need to carry out legitimate Company activities that are directly related to the permitted use of the ID Card numbers.

Employees permitted to access those ID Card numbers must take all reasonable steps to ensure that ID Card numbers are never publicly displayed alongside the name of the relevant Customers.

(b) Disclosure of Customer Data

The Company and its employees must not disclose any Customer Data to any third party, whether in person, by telephone or email/messaging, in social media or in other communication, unless either:

- the Customer's **prior** consent has been obtained; or

- the disclosure is necessary in order for the Company to provide the Customer with our services; or

- the disclosure is required by Applicable Law, in which case the Legal Department should be consulted in advance (legal@lcjgroup.com), if that type of disclosure has not already been approved by them.

(i) Disclosures by consent:
In order to have appropriately received consent to the disclosure of a Customer's Data to a third party, employees should obtain a **written** direction from the Customer allowing the disclosure of their Customer Data, either generally or for a specific purpose and/or to a specific person.

Before actually disclosing any Customer Data to the third party specified under a Customer's written consent, employees must first verify the identity of the specified third party (for example, by checking some form of personal identifying information of the recipient).

If employees have any doubt whether or not to disclose the Customer Data, they should first obtain authorisation from the Legal Department, as a Data Privacy Officer for the Company in Hong Kong.

(ii) Disclosures necessary to provide Customers with services:
It is often the case that in order to provide Customers with services they request, the Company needs to disclose certain Customer Data to third parties, such as to vendors or delivery companies. For these service purposes, the Company must:

- use reputable third parties that commit to protecting Personal Data in accordance with Applicable Law; and

- keep proper records of the Personal Data given to such third parties.

When entering into contracts that allow third party access to Customer Data, employees must ensure those contracts require the third party to comply with all data protection requirements under Applicable Law. The Company's **standard data privacy undertaking** must be included in all such contracts – if any employee does not have a copy of that undertaking, please ask the Legal Department for it.

If the third party refuses to agree to the undertaking, please consult the Legal Department promptly. Please note: the **contract cannot be signed** until approved by Legal.

(c) Customer Data direct marketing opt-outs

At the time Customer Data is provided to the Company, the Customer should be given the option to "opt-out" from receiving any future direct marketing communications from the Company, by not ticking the "opt in" box on the Company's data collection form. The Customer may also opt-out of those communications at any later time, via the Company's websites or otherwise in writing to the Company.

Employees must not use the Personal Data of Customers who opt-out (as above) to contact the Customer for any future sales or marketing purposes. Those Customers will be clearly tagged on the Company's customer relationship management (CRM) system. Relevant employees must ensure that the correct 'consent to direct marketing' information is entered in the Company's CRM sequence for generating direct-marketing Customer mailing lists.

Any "opt-out" requests received from Customers at a later time should be passed to the Company Concierge or Customer Care team of the Company, who must update the Customer's record in the CRM system and implement the change with immediate effect.

No transfer of Personal Data belonging to Customers who have "opted-out" (as above) may be made to any other person, organisation or party for sales or marketing purposes, including to any other part of the Company or any other company that owns it or is under common control with it.

(d) Compliance with "Anti-Spam" laws when using Customer Data

Employees must comply with the laws relating to "Unsolicited Electronic Messages" in Hong Kong (summarised in the next paragraph) when sending commercial electronic messages *(* SMS/MMS), social media or fax. In particular, employees must not send messages to a number listed on the HK Communications Authority's "do-not-call" registers unless prior consent from the Customer is obtained.

When sending electronic messages to Customers not on those registers, employees must

- provide accurate sender information in the header of any written message, in English and Chinese;

- not conceal or withhold any caller display or message sender identification;

- not use a misleading subject heading for a written message;

- provide an unsubscribe function in any written message, clearly and conspicuously in both English and Chinese; and

- ensure that any unsubscribe requests received from a Customer are recorded in the Company's CRM system by no later than 10 working days from the day the Customer sends the request to the Company.

(e) Safeguards for protection of Customer Data

(i) Use of the Company's CRM system:
Only employees who have an authorised Company CRM login ID and password may access the Company's CRM system and its Customer Data. Customer Data access, extraction, alteration and other use rights are limited to only those employees for whom it is necessary for the purposes of their Company role. Those employees may only access or use that Customer Data for the purposes of that role. Please note that such rights are promptly removed on employment termination.

The above employees must keep their CRM system details secure and not share them with anyone other than Executive Management (please see the definition of Executive Management in the Introduction to this Part B of the handbook) or their Line Manager, or, for remedial purposes, an authorised member of the Tech/IT Department.

(ii) Hard copies of Customer Data
To further protect Customer Data, employees with access to it must ensure that any hard copy form of it is not left unattended or accessible to others in offices or stores, but rather is locked in desks, cabinets or counters when not in use and is shredded before any disposal of it.

In addition, relevant employees must ensure that keys or key cards are required for access to offices and stores outside of business hours and that visitors will not be permitted to walk unattended in areas of Company premises where Customer Data is accessible.

(f) Retention and destruction of Customer Data

Unless it obtains the specific consent of **the** Customer, the Company may not retain Customer Data for longer than is necessary to fulfil the collection and use purposes notified to the Customers at the time their Customer Data was collected.

Upon expiry of the applicable retention period and confirmation from the Legal Department, authorised employees may permanently destroy the Customer Data as follows:

(i) if the Customer Data is in hard copy form, by shredding and then securely disposing of it; and

(ii) if the Customer Data is in electronic form, by permanently erasing it from the Company's systems in cooperation with the Tech/IT Department.

(g) Customers' access to their data and complaints of misuse

Customers are entitled to ask if the Company holds Personal Data about them, to access a copy of any such Personal Data and, if inaccurate, to have it corrected by the Company. Any such Customer requests received by an employee must immediately be sent for handling to the Legal Department (legal@lcjgroup.com), as a Data Privacy Officer for the Company in Hong Kong.

Unless the Company declines an access request, access will be effected within 40 calendar days, in a reasonable manner and in an understandable form. The Company may charge a reasonable fee for providing it. If the Company refuses an access or correction request from a Customer, we must provide the Customer with our reasons. The Customer is entitled to object to our refusal.

If an employee receives a complaint alleging misuse of Customer Data, the complaint must also be referred immediately to the Legal Department (legal@lcjgroup.com), as a Data Privacy Officer for the Company in Hong Kong.

(h) Response to Customer Data security breach

The Company has a Data Incident Response Plan (**"Plan"**) that sets out how the Company may manage loss, erasure, breach, unauthorised or accidental access, processing, damage and/or alteration of any Personal Data ("**Data Incident**"). The Plan comprises a four-step approach for dealing with the relevant Data Incident, namely: (1) **identification**, (2) **assessment**, (3) **response** and (4) **notification and review**. The Plan can be accessed at any time from the Legal Department or the Tech/IT Department.

Applicable Law may require the Company to notify Hong Kong's Privacy Commissioner of Personal Data and/or other authorities of the security breach. Employees must immediately assist the Legal Department of the Company with any legal investigation into the breach and notification (if applicable). The Legal Department will determine whether any notifications of the security breach should also be made to Customers under Applicable Law or policy.

Employees who discover any actual or suspected security breaches or who are asked to assist the Company in containing or remedying any such breach must also promptly contact the Legal Department (legal@lcjgroup.com) to determine the extent and manner of documentation to be prepared in respect of the security breach and the Company's remedial measures.

7.4 Company's Collection and Use of Third Parties' Personal Data

The Company will treat all Personal Data held by it that belongs to a third party:

(i) as Confidential Information (subject to applicable clauses of any contract with that third party) and;

(ii) with the same care as employees' Personal Data under this Protection of Personal Data Privacy policy and in accordance with Applicable Law.

7.5 Violations of this Policy

All employees are responsible for ensuring that they comply with the procedures outlined in this Protection of Personal Data Privacy policy. Any employee who becomes aware of a violation of this policy must promptly report any such violation either to the Human Resources Department or the Legal Department (legal@lcjgroup.com), as Data Privacy Officers for the Company. Intentional or negligent breaches of this policy may result in disciplinary action, including termination of employment.

7.6 Further information

As noted earlier in this policy, if employees have any questions about this Protection of Personal Data Privacy policy or about data privacy generally, they should feel to contact the Legal Department (legal@lcjgroup.com), as a Data Privacy Officer for the Company in Hong Kong.

Our Principles: We Act with Integrity

8. ANTI-CORRUPTION

Please note: this Anti-Corruption policy is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or any separate agreement.

Reason For This Policy: The Company is committed to promoting a culture of integrity, incorruptibility and fair dealing in everything we do.

8.1 Zero Tolerance of Corruption

It is the Company's policy to conduct all business in an honest and ethical manner. The Company takes a **zero-tolerance approach** to all corruption, including bribery, and is committed to acting professionally, fairly and with integrity in all business dealings and relationships wherever the Company operates.

.

The Company is also committed to implementing and enforcing effective systems and procedures to prevent, detect and remedy bribery, as well as to take disciplinary measures against any of its employees who engage in it.

8.2 Bribery

(a) What is a bribe?

A bribe is the offering, giving, promising or authorising the payment of **anything of value** (including cash, gifts, entertainment, services or any other benefit) to **any** individual or entity **in exchange for** obtaining any commercial, contractual, regulatory or personal advantage from that individual or entity.

Anti-bribery laws are generally consistent in all of the countries in which the Company operates. We have summarised those laws below. However, to the extent that this policy and any local anti-bribery laws conflict, the more stringent of the standards will apply.

The main offences under applicable anti-bribery laws in the countries in which the Company operates include:

- Giving a bribe to any individual, entity or organisation
- Giving a bribe to any government, quasi-government entity or other entity or organisation affiliated with a government
- Receiving a bribe either for himself/herself or on behalf of another person
- Giving or receiving a bribe indirectly through another person, entity or organisation

The **Company** can also be liable if bribery offences are committed by its employees or any third parties acting on behalf of or for the benefit of the Company. Such third parties can include our Business Partners, agents or other people or organisations acting either on our behalf or as an intermediary for us.

Some common examples of bribery are set out at the end of this anti-bribery section.

(b) Bribery is prohibited

The Company **prohibits the offering, giving, requesting, authorising or accepting of bribes**. Bribery is prohibited in whatever form it takes, and regardless of whether it involves private persons, government or other public officials, incorporated entities, unincorporated businesses or other organisations.

The Company also prohibits the making or acceptance of so-called **'facilitation payments'** or **'kickbacks'** of any kind.

- ***Facilitation payments*** are typically small, unofficial payments of money made to secure or speed up a routine government action by a government official, such as the granting of a business visa or the clearance of goods being imported into a country. In some countries in which the Company operates, third parties such as customs agents or border staff may try to persuade our employees that facilitation payments are a common "unofficial" practice in that country. However, please note that these payments are **prohibited** under local anti-bribery laws and, regardless of any local practices that may turn a blind eye to them, they will **not be tolerated** by the Company. If any employee is asked to pay one of these facilitation payments, they should decline to do so and immediately notify their Line Manager or their HR representative.

- ***Kickbacks*** are typically payments made in return for a business favour or other advantage, when an **unearned** sum is added to a legitimate payment and paid to the person who is granting the favour or advantage. **A common example** of a kickback is the situation where an employee agrees to a supplier's invoice that charges a higher rate for a product or service than is usually paid in the market, with that employee then receiving a payment (i.e. the kickback) from the supplier in return for the acceptance of that higher invoice.

Employees must avoid any activity that might lead to a facilitation payment or kickback being made by the Company or that might suggest that these types of payment are acceptable to the Company or its staff.

If employees are asked to make or approve a payment on the Company's behalf, they should always consider what the payment is being made in return for (e.g. goods or services) and whether the amount requested is **appropriate and proportionate** to the goods or services being provided for that payment.

When making or approving a payment on the Company's behalf, employees should also always ask for a **written receipt** that sets out in detail the goods or services that have been received for the payment.

If employees have any concerns or queries regarding payments in this respect, please raise these with **the** Legal Department immediately (legal@lcjgroup.com).

(c) Some examples of bribery

(i) Offering a bribe:
A Company employee offers a potential client a ticket to a prominent fashion event, but only if the client agrees to do business with the Company.

This is a bribery offence, because the employee is making the offer of tickets **in order to gain a commercial and contractual advantage**. The **Company** may also be found to have committed an offence, because the offer has been made to *obtain* business for the Company. It may also be an offence for the potential client to accept the (bribery) offer.

(j) Receiving a bribe:

A vendor offers a Company employee's nephew a job, but makes it clear that, in return, the vendor expects the employee to use their influence in the Company to ensure that the Company does (or will continue to do) business with that vendor.

It is an offence for the vendor to make such an offer. It is also an offence for the **employee** to accept the offer, because the employee would *be* doing so to gain a personal advantage.

8.3 Corrupt Acts of Third Parties

(a) Corruption by business representatives

In certain circumstances, the Company can be held responsible for the actions of a third party who acts for or on behalf of the Company, such as agents/agencies, brokers, consultants, contractors, distributors, service providers and joint venture partners. To help protect the Company in this regard, employees must ensure that any third party they use in the course of their employment is only engaged for **legitimate business purposes on an arm's-length basis** (i.e. at market price and on commercially standard, reasonable terms) and is only paid for the legitimate provision of goods and services in accordance with those terms. All engagements with third parties must be **documented in a written agreement**, which agreement must be reviewed and approved by Legal and fully signed **before** the engagement starts.

Employees may only agree to a discount, rebate, commission, success fee, bonus or other similar arrangement being awarded to a third party **if** (i) it is commercially reasonable and (ii) it is being awarded in exchange for the legitimate provision of goods and services in accordance with the written engagement agreement.

Employees engaging third parties must use their best efforts to perform reasonable **due diligence on those parties** to ensure that the third parties are reputable, solvent and will not wrongfully offer, provide, receive or solicit anything of value on behalf of the Company in connection with the Company's business.

Employees must also regularly monitor their relationships with such third-parties for compliance with this policy. **Any** violations or other issues uncovered during the course of a third party relationship should be promptly reported to the Legal Department (legal@lcjgroup.com).

(b) 'Passing off' and parallel imports by customers

Employees must report to their Department head or Executive Management (please see the definition in this handbook's Part B Introduction), any purchase by an individual Customer of:

- more than ten items of the same cosmetic item; or
- more than five items of the same item of non-cosmetics merchandise that is valued at over HK$10,000 per item.

This is to protect the Company from the risk of some Customers illegally exporting the purchased merchandise to higher tax jurisdictions for re-sale.

8.4 Other Potential Red Flags

The following are some other possible red flags that could raise concerns under this Anti-Corruption policy.

This list is not exhaustive and is for **illustrative purposes only**. If employees encounter any of these or similar scenarios, they should promptly report the situation to their Department head or the Human Resources or Legal Departments.

- An employee becomes aware that a third-party business contact that engages in, or has been accused of engaging in, improper business practices;
- An employee learns that a third-party business contact has a reputation for paying bribes, or for requiring that bribes be paid to their staff, or has a reputation for having a "special relationship" with government officials (of any country) which seems to lead to business advantage;
- A third-party business contact insists on receiving a commission or fee before committing to sign a contract with the Company or to carry out a government function or process for the Company;
- A third-party business contact requests payment in cash and/or refuses to sign a formal agreement with the Company or to provide an invoice or receipt for a payment made;
- A third-party business contact requests that payment is made to a country or geographic location different from where the third party resides or conducts business;
- A third-party business contact requests an unexpected additional fee or commission to "facilitate" a service;
- A third-party business contact requests that a payment is made to "overlook" potential legal violations or issues;
- An employee receives an invoice from a third-party business contact that appears to be non-standard or customised;
- An employee notices that the Company has been invoiced for a commission or fee payment that appears large when measured against the market rate and/or service provided;
- A third-party business contact appears to lack the qualifications and resources to perform the services offered;
- A third-party business contact gives a guarantee of success;
- A third-party business contact requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to the Company or that does not appear to be responsible for doing anything in return for its fee.

8.5 Who to Contact to Raise Concerns or Seek Guidance about Corruption

(a) Primary contacts

We have listed below the people or Departments who are primarily responsible for different parts of this Anti-Corruption policy. Employees should contact them promptly if they have concerns about, or need guidance on, those Anti-Corruption aspects:

- The Legal Department (legal@lcjgroup.com) in respect of the implementation and enforcement of appropriate procedures to reflect the Anti-Corruption policy and for reporting relevant matters of concern to the Board of Directors of the Company.

- The Human Resources Department in respect of the reflecting of the policy's requirements in employment contracts and updated versions of this handbook, as well as the establishment of appropriate training on this policy.

- The Corporate Finance Department (CorpFinancePolicies@lcjgroup.com) in respect of the communication of this policy to all Business Partners and the inclusion of its principles in standard terms of business and contracts.

Please remember: all employees are responsible **for compliance with this policy.**

(b) Alternative contact

If any employees have concerns or queries regarding possible bribery or other corruption, they may additionally or instead raise them with the Legal Department (legal@lcjgroup.com).

Employees are encouraged to raise concerns about any instance of possible corruption at the earliest possible opportunity. Please also see the Whistleblowing policy contained in this handbook.

9. INTERNAL FINANCIAL WRONGDOING

Reason For This Policy: Acts of financial wrongdoing, such as fraud, theft and unauthorised or unlawful payments, that are effected or facilitated by individuals **within** the Company significantly damage the Company's business. These behaviours are also acts of corruption. They are **prohibited**.

9.1 Please Speak Up

Employees should be aware that acts of financial wrongdoing, such as those listed above, do occur within workplaces. They cause serious harm. Any employee who encounters any such wrongdoing at, or in connection with, the Company **must** speak up about it. Such employees should immediately contact one or more of the following people or Departments: their Department head, the Legal Department (legal@lcjgroup.com), the Corporate Finance Department (CorpFinancePolicies@lcjgroup.com) or any member of Executive Management (collectively, the "**Reporting Group**").

Some examples of financial wrongdoing, and how it may be spotted, are listed in the Fraud section below.

9.2 Fraud

(a) Examples of internal fraud

There are many types of internal company fraud, including:

- Theft by way of an employee's skimming of sales revenue or misuse of company assets, such as using a company credit card to pay for personal expenses;
- Embezzlement via the padding of employee expense reports or the submission of fake vendor invoices by an employee;
- Accounts Payable fraud, such as "pay and return" schemes, where an employee causes or allows the Company to overpay a vendor, asks the vendor for a refund of the overpaid amount and then uses that refund for their own purposes;
- Accounts Receivable fraud, such as where an employee is using customer funds for their personal use and, to avoid being caught, uses funds in one of the Company's bank accounts to cover the funds stolen from another;
- Privileges fraud, such as where employees use for themselves the membership points, membership status or other benefits that customers have accrued as part of a Company membership/privilege programme;
- Vendor fraud, such as kickbacks and bribery; and
- Payroll fraud.

(b) Be aware

We ask that all employees be alert to suspicious financial activity **within** the Company, such as:

- invoices or expenses charged to the Company that appear inflated in price or are not accompanied by the correct approvals or documentation;
- tenders that seem always to be won by the same bidder;
- multiple service providers or vendors using the same address;
- former employees or employees' relatives being connected to a vendor or other service provider to the Company;
- colleagues who have become very reluctant to share their processes or to have someone review the contracts or invoices for which they are responsible; or
- frequent tips or complaints being received about a particular colleague.

If employees see anything in this respect that appears suspicious or otherwise not right, please contact any member of the Reporting Group (above) **as soon as possible**.

9.3 Business-related Expenses

Each Business Group's Finance Department has a detailed policy on business-related expenses, whether those expenses are incurred locally or while on business travel. We have extracted only **some** parts of the guidance from those policies here. Employees must ensure they understand and comply with their respective Business Group's full policy.

(a) Eligibility for payment/reimbursement of expenses

Employees must settle all Company-related expenses by corporate credit card, if available. Only those expenses that are (i) business-related and (ii) appropriately documented and submitted via the relevant Company expense reporting form will be eligible for reimbursement by the Company.

Please note that in order for the Company to allow entertainment expenses to be categorised as a business deduction under applicable tax regulations, employees must clearly state the cost, business purpose and name and title of each guest in their expense reporting form, and attach an appropriate receipt wherever possible. If an employee (or their Line Manager) does not have this expense reporting form, they should obtain it from their Business Group's Finance Department.

(b) Reporting of expenses

All expenses incurred by employees on behalf of the Company, including for business-related gifts and hospitality (please see below), must be promptly and accurately recorded in accordance with the Company's requirements then in force.

(c) Service charges and tips

Employees' payment of a service charge on restaurant bills for approved business hospitality purposes is permitted, but additional tips may only be paid if the situation renders it necessary or desirable. Tips from multiple bills must not be presented as one lump sum in the Company reporting form; each expense should be separately listed and described in the form.

Each Finance Department's business-related expenses policy sets out limits on the service charges or tips that staff are permitted to pay for business purposes. Staff must read and comply with their respective policy's limits. Service charges or tips above those limits will not be reimbursed by the Company.

(d) Wrongful expense claims

False or inflated expense claims constitute **corruption and a fraud against the Company**. They are strictly prohibited and may lead to disciplinary action, potentially including summary dismissal by the Company, without compensation to the employee, and/or **criminal** proceedings.

9.4 Business-related Gifts & Hospitality

From time to time an employee may be asked to accept a gift or an offer of hospitality from a Business Partner. Conversely, an employee may feel it is required or appropriate to offer a gift or hospitality to a Business Partner. In this context, "**hospitality**" includes meals and/or drinks with the Business Partner, event tickets and other entertainment activities, as well as related items such as flights, other transport or accommodation.

This policy explains the restrictions on **the type and value of gifts and hospitality that can be accepted or offered by employees** in connection with the business of the Company.

(a) General principles:

(i) With the limited exception of a small amount of Lai See (or similar), please note that **cash or a cash-equivalent** (such as gift cards or coupons) should **never** be given or received in connection with the business of the Company.

(ii) With the approval of their head of Department, an employee **may** offer to a Business Partner, at the Company's expense or reimbursement, a **small gift or reasonable hospitality** that is both:

- limited in value (please see the relevant Finance Department's policy); and
- offered for a valid business purpose in accordance with the applicable policies.

If any employee does not have a copy of the relevant policy, they should obtain it from their Business Group's Finance Department.

(iii) In the same way, employees **may accept from** a Business Partner **a small gift** (e.g. promotional items of a low value, such as a branded umbrella or a packet of Lai See envelopes) **or reasonable hospitality** that is limited in value and given for a legitimate business purpose, provided that the employee's head of Department approves that gift or hospitality. In respect of business-related **hospitality** being offered **to** a Business Partner **by** an employee, please also see the section entitled "Further guidance re hospitality" below.

(iv) No employee may offer or accept an offer of a gift or hospitality that is worth more than HK$1,500 (or the equivalent in the relevant local currency) in value. If a gift worth more than HK$1,500 is offered to an employee, the employee must immediately notify their Line Manager.

(v) Similarly, employees **must not** offer or accept hospitality or gifts to or from a Business Partner that, although possibly difficult to value, are **lavish or are repeated**. Lavish or repeated offers received by an employee must be reported to the employee's head of Department and the Human Resources Department.

(vi) Gifts offered or proposed to be accepted during traditional holidays (such as mid-Autumn festival, Christmas or Lunar New Year) should also be modest in amount, reasonable in terms of the relationship and only made under appropriate circumstances.

(vii) Any gift or hospitality should be tasteful, respectful and not have the potential to adversely impact the Company's reputation or business and community relationships. In particular, employees should not offer or accept gifts or hospitality that would violate any Applicable Law.

(viii) Gifts and hospitality must be given and received transparently and must be accurately documented in the Company's records. The Corporate Finance Department will provide other departments with a template for this required documenting.

(ix) Employees are obliged to communicate our gifts and hospitality policy to their contacts from Business Partner organisations to avoid miscommunications or other awkward situations with Business Partners in this context.

(x) If any employee or their Line Manager feels it is professionally inappropriate to decline a significant offered gift or hospitality, or repeated offers, the offer(s) should be reported to the employee's head of Department **and** the Human Resources Department and the details of it recorded. The head of Department and the Human Resources Department will then jointly decide whether the offered gift(s) or hospitality should be either declined by the Company, kept by the employee or accepted by the Company and then donated for charitable purposes.

(b) Further guidance re gifts

During Lunar New Year, all Lai See or "red packets" **received** by employees due to business dealings should be reported to the Department Head (except those mutually offered amongst colleagues). Lai See valued over HK$200 (or the equivalent amount in the relevant local currency) should be passed to the Company for donation to charitable organisations.

Employees may **offer** Lai See to Business Partners, **provided that** the amounts given are nominal in value and in line with custom and tradition. They should not exceed HK$200 (or the local equivalent) in value.

(c) Further guidance re hospitality

Reasonable hospitality is regarded as an acceptable form of business and social behaviour, including paying for a business contact's food or drink for consumption on the occasion when it is provided, for entertainment events (e.g. concert/theatre/sports tickets) and activities connected with them, such as transport to or from them. However, staff should be aware that hospitality and entertainment activities are open to being exploited for corrupt or otherwise unethical purposes. Accordingly, the following additional principles apply in relation to employees **offering or receiving hospitality in the course of Company business**:

(i) All entertainment expenses must be business related. For further guidance in this respect, please see the section "Business-related Expenses" above.

(ii) The Company will not reimburse the purchase by employees, at any level, of alcohol for business entertainment purposes, unless the expenditure has been specifically authorised in advance in accordance with the policies of the employee's respective Finance Department.

(iii) The cost of hospitality related to an approved Company-budgeted event should be allocated only against that event's budget -- e.g. a dinner for guests at a PR launch or promotional event should be accounted for under the **event budget**, **not as an entertainment expense**.

(d) Gifts for business contact friends

The Company recognises that employees, colleagues and Business Partners may also become friends outside of work. Mutually offering gifts on special occasions (such as birthdays, holiday festivals, job departures or retirements) is acceptable, but employees should note the following:

- These gifts should be paid for by the individual offering them, not paid for or reimbursed by the Company or the Business Partner's organisation; and

- Employees should promptly inform their head of Department or a member of the Human Resources Department of any issue arising from these personal relationships.

9.5 Charitable Contributions

As part of the Company's Corporate Social Responsibility commitment, the Company currently supports several charitable causes. Any proposed charitable donation to be made by the Company or otherwise using Company funds must be for a legitimate purpose and not conditioned upon receiving business or other benefits.

Charitable contributions are also subject to the following guidelines:

- The contribution must be made with the sole purpose of furthering the recipient's charitable or philanthropic mission;

- The circumstances of the contribution should not be able to be reasonably perceived as an improper attempt to influence or reward any individual, including a government or public official, in connection with the Company or its business; and

- The contribution must be properly documented and approved in advance by a member of the Company's Executive Management (please see the definition of Executive Management in the Introduction to this Part B of the handbook).

9.6 Political Contributions

Political contributions are donations to a political campaign, party, official or candidate, or any other organisation that supports or promotes political views. Political contributions using Company funds or in the Company's name are prohibited, unless authorised by the Board of Directors of the Company.

9.7 Who to Contact to Raise Concerns or Seek Guidance about Internal Financial Wrongdoing

If any employee discovers any activity that may constitute financial wrongdoing within the Company, including **theft, embezzlement, Company accounts manipulation or other fraud**, they **must immediately** report it to a member of the Reporting Group (above). That person must then investigate the matter and report it as appropriate.

As far as practicable, the Company will treat all information received from any employee about internal wrongdoing as **confidential** and will take necessary steps to protect the rights of that employee. All reports honestly made will be regarded as necessary in safeguarding the Company's interest.

9.8 Responsibility for Internal Financial Wrongdoing Policy

The head of the Corporate Finance Department has ultimate responsibility for implementing and enforcing the Internal Financial Wrongdoing policy and, along with the Legal Department, for reporting to the Board of Directors of the Company in respect of these matters.

The Human Resources Department is responsible for establishing appropriate procedures within their operations in this regard and for reflecting the policies' requirements in employment contracts and updated versions of this handbook.

The Corporate Finance Department is responsible for ensuring that the principles of this policy are communicated to all Business Partners and included in standard terms of business and contracts.

Please remember: all employees are responsible for complying with these policies. **Please report to any member of the Reporting Group (above) any wrongdoing within the Company that you see or reasonably suspect**. As we mention above, as far as is practicable in the context of the specific

investigation, the Company will treat all information received from any employee about internal wrongdoing as **confidential** and will take necessary steps to protect the rights of that employee.

10. CONFLICTS OF INTEREST AND OUTSIDE WORK

Please note: this Conflicts of Interest and Outside Work policy is contractual in its effect and applies **in addition to** any other obligations under an employee's employment contract or separate agreement.

Reason For This Policy: A conflict between an employee's interests and the interests of the Company -- whether an actual, potential or perceived conflict of such interests -- may harm the Company's operations, relationships, reputation or other business aspects. Accordingly, all employees of the Company, regardless of their level or seniority, are expected to act in the Company's best interests and avoid situations that create any such conflict of interest, including those that may arise as a result of employees performing work outside the Company.

10.1 Employee Conflicts of Interest

An employee conflict of interest generally arises when the employee (or a person close to them, such as a member of their family, a personal partner, a close friend, etc.) has a personal, monetary or business interest or motivation that:

- interferes with the employee's ability to make sound, objective business decisions on behalf of the Company; or

- otherwise compromises the employee's judgment, decisions or actions in the workplace or simply in the role that the employee performs in the Company—e.g. a role where the employee has access to confidential information of the Company and consequently has a duty not to improperly disclose it.

Despite the best of intentions, harm can be caused to the Company by even a **potential** conflict of interest or by a situation that is only **perceived by others** to be a conflict of interest.

Consequently, all employees must avoid actual, potential or perceived conflicts of interest with the interests of the Company, whether (for example) in their business relationships with their colleagues (such as reporting into or managing a Close Contact in a work context), their dealings with Business Partners, Customers or competitors of the Company or their interactions with other organisations or individuals seeking to do business with or to compete with the Company.

Please be aware that for these purposes:

- "**actual, potential or perceived conflicts of interest**" also include any conflicts of interest that an employee's close relations, personal partner or anyone who regularly lives in that employee's usual home residence ("**Close Contacts**") may currently or **potentially** have or that they may **appear** to have; and

- "**close relations**" (as used in the paragraph above) include:

    - an employee's parents, siblings, grandparents (and any similar relations by marriage – e.g. a step-brother); and

    - any siblings of the employee's parents (i.e. the employee's aunts/uncles) and an employee's cousins.

A note re "seasonal staff": As with all staff, the Company expects employees who have been advised that their employment is seasonal in nature ("**Seasonal Staff**") to use their best efforts to avoid situations that may create a conflict between their activities and the business interests of the Company. However, the Company does not require those Seasonal Staff to complete the conflicts of interest declaration form that is mentioned below in this policy.

10.2 Employee Declaration of Conflicts of Interest

As a result of the above, on the commencement of employment by any employee, other than Seasonal Staff, who is being hired by LCJG for more than one month ("**Eligible COI Staff**"), such employees must declare to the Company, in the form provided by it (the "**COI Declaration**"), all **actual, potential or perceived conflicts of interest**.

The COI Declaration is to be completed and returned by Eligible COI Staff at the start of each such staff-member's employment with the Company and at any other time reasonably requested by the Company. Members of the Company's senior team or those staff who hold certain other positions or in certain departments maybe asked to complete the COI Declaration annually.

Other than via the COI Declaration, all Eligible COI Staff **must also** declare to the Company any actual, potential or perceived conflict of interest that arises in the future, **as soon as that conflict is known to that employee**.

The Company reserves the right to follow up with any Eligible COI Staff on any information provided to it in this regard, including to request the relevant employee to provide more detailed information and/or to take appropriate steps to remove or mitigate the conflict.

10.3 Some Examples of Conflicts of Interest

Although it is impossible to list every situation that could create a conflict of interest between employees and their employing company, the following are examples of situations that employees or their Close Contacts may find themselves in and which may be deemed an actual, potential or perceived conflict of interest if any of those situations arise during the employee's employment. Please note these are only **examples**; they are not an exhaustive list of all potential conflict of interest situations.

- Being directly or indirectly involved on a personal basis in business dealings with the Company or any part of it – e.g. an employee or their Close Contact having a business interest in a company that is, or is seeking to be, a vendor of goods to the Company;

- Being directly or indirectly involved in any dealings with Business Partners, Customers or competitors of the Company in a way that could be seen as the employee or the Close Contacts **competing** with the Company – e.g. an employee's cousin's business pitching for the right to sell a vendor's products that are currently sold by the Company;

- Granting or guaranteeing a loan to, or accepting a loan from or through the assistance of, any Business Partner or competitor of the Company;

- Without the prior written approval of the Company, having a Close Contact who works at the Company in a direct reporting relationship with the employee or where either the employee or the Close Contact is the head of the Department in which they both work;

- Without the prior written approval of the Company, taking on certain concurrent work outside the Company, either on a regular or a consulting basis. For further details about this type of potential conflict of interest**, please see** the Company's requirements in relation to "Outside Work", below;

- Engaging in any gambling of any kind (including in card games and games of mahjong) with persons who have business dealings with the Company. Please note that in social games with Business Partners, Customers or potential business contacts (again such as card games and games of mahjong), employees must exercise caution and good judgment; they must withdraw from any such games in which money, items or other value is at stake.

- Holding any interest in any third party company or organisation which:

    - is or is seeking to be in competition with any business carried on by the Company; or

    - is or is seeking to be in business dealings with the Company; or

    - might reasonably be thought by the Company to harm the employee's ability to act at all times in the best interests of the Company; or

    - might reasonably be thought by the Company to require the employee to disclose any of the Company's Confidential Information,

    except that the holding by an employee (or Close Contact) of any shares or financial securities in any third party company that is **publicly listed** on a recognised investment/stock exchange or securities market will **not** be deemed a conflict of interest for the purposes of this policy, **if** that holding does not exceed 5% of the total shares or other securities in that public company.

10.4 Failure to Declare Conflicts of Interest

As with other breaches of this handbook, the failure by Eligible COI Staff to declare an **actual, potential or perceived** conflict of interest could result in the Company taking disciplinary action against the relevant staff-member, potentially including termination of employment.

Please remember: the requirement to inform the Company of any conflict of interest is a continuing obligation. As a result, Eligible COI Staff should kindly notify the Human Resources Department if they have any actual, potential or perceived conflict of interest arise in the future.

10.5 Conflicts of Interest and Outside Work

As the Company continues to grow, so does our pool of talent. The Company recognises that, during their employment, some staff may want to explore additional avenues to develop their skills and capabilities in new ways, including through working outside the Company.

While we do not want to inhibit such personal growth, the Company needs to protect itself against conflicts that may arise between its interests and the interests of relevant employees in respect of contemporaneous Outside Work (defined below). Accordingly, the Company has put in place certain requirements relating to Eligible COI Staff (defined further above), depending on whether the relevant staff-member wishing to take on the Outside Work is employed by the Company on a full-time or non-full-time basis. Please note that the Outside Work requirements do not apply to Seasonal Staff.

For the purposes of this policy, "**Outside Work**" means working for, or providing services to, outside companies, organisations or individuals, **whether on a paid or unpaid basis**, **except for private** tutoring work in respect of academic subjects and unpaid work for **charitable, environmental or community** causes.

(a) Full-time Eligible COI Staff

Full-time Eligible COI Staff must not take on Outside Work **if that work could conflict** with either the relevant staff-member's work for the Company or the operations of the Company generally.

Because of the potential for conflicts of interest that Outside Work can cause, the Company requires that any full-time Eligible COI Staff who wish to undertake such Outside Work must **apply** to the Human Resources Department, a reasonable period of time in advance, for approval of the proposed Outside Work, setting out the full details of it.

The Human Resources Department will review those details and advise the employee, within one month of receiving the application, whether the requested Outside Work is approved. Approval of Outside Work is at the absolute discretion of the Company.

(b) Non full-time Eligible COI Staff

We also ask that **non full-time** Eligible COI Staff declare in the COI Declaration if they perform any Outside Work.

However, because non full-time Eligible COI Staff might have multiple other jobs outside the Company, we require **only** that those staff-members **declare** this Outside Work; they do not have to seek the Company's prior **approval** of it.

If the Human Resources Department then considers there is likely to be a significant conflict between any declared Outside Work and the interests of the Company, it will contact the relevant employee to discuss the declared work, as well as the options available in that situation.

Please note:

- These Outside Work rules also apply to any provision of services to or participation in events that an employee is invited to perform by an outside party as a result of the employee's work expertise.

- The requirement for Eligible COI Staff to inform the Company of Outside Work is a **continuing obligation**. As a result, Eligible COI Staff should kindly notify the Human Resources Department as soon as possible if they intend to take up any Outside Work in the future.

10.6 Private Transactions

Private transactions on the Company's premises between employees and any Business Partner or customer of the Company are **not** permitted.

11. FAIR BUSINESS PRACTICES & COMPLIANCE WITH COMPETITION LAW

Reason For This Policy: As a competitor in a global marketplace, the Company has a strong interest in protecting the fairness of that marketplace for all. Honest and equitable business practices, including strict compliance with applicable "competition laws", are key aspects of the fair marketplace from which we benefit.

11.1 Scope of Competition Law Obligations

Competition Law (also often known in some places as "Antitrust Law") aims to protect the competition in markets so as to maximise fairness to consumers. Potential breaches of Competition Law by companies include:

- "Anti-competitive" agreements between companies, such as agreeing to: raise prices together, put their products on sale at the same time, mutually plan their product launches or set similar discount levels;
- Exchanging sensitive price information with competitors
- Abusing a dominant position that a company has in the market or some other substantial degree of market power.

In Hong Kong, breaches of Competition Law have serious consequences, including:

- heavy fines;
- reputational damage;
- the Company's commercial agreements being ordered to be unenforceable;
- third parties who have suffered loss (including Customers) bringing legal actions against the Company for damages by third parties; and
- disqualification of Company directors.

We have set out guidance on some key aspects of Competition Law in the rest of this section, but this guidance is **merely an overview** of the key aspects of Competition Law requirements. The Company provides further, more detailed training on Competition Law for relevant employees, including antitrust protocols for those employees, and the Legal Department is always available to discuss any Competition Law concerns or questions that any employee has – please email legal@lcjgroup.com or otherwise consult your usual contact in the Legal Department.

11.2 Anti-Competitive Agreements

Generally speaking, anti-competitive agreements are arrangements which may harm competition or potential competition in a way that Competition Law authorities consider to be unfair. Some examples are explained below.

(a) Agreements with competitors

Agreements between competitors that harm competition are prohibited under Competition Law and lead to severe penalties. An "agreement" for these purposes has a very wide meaning and while it includes written contracts, it also includes non-written arrangements, such as oral agreements and even implied or "tacit" understandings.

Employees must not reach **any** sort of agreement or understanding with a competitor about any aspect of the Company's current or future behaviour in the marketplace. This includes agreements to:

- Fix, raise or lower prices or keep them at a similar level (called "stabilising" a price);
- Fix other competitive terms, such as margins, commissions, fees, discounts or credit terms;

- Allocate markets, Customers, suppliers or geographic territories between each other;
- Fix, control, prevent, limit or eliminate the production or supply of products or services;
- Collude with a competitor in response to an invitation to tender; or
- Limit competition in any other way.

(b) Agreements with Business Partners

Competition Law also extends to agreements with suppliers, distributors and other Business Partners if those agreements are likely to harm competition. For example, employees must not reach **any** sort of agreement or understanding with a supplier or distributor to:

- Fix or set the minimum price at which the Company or any party to the agreement must re-sell a product; or
- Fix or set the timing of price increases or discounts.

11.3 Exchanging Information with Competitors

Sharing non-public, commercially sensitive information with a competitor may also infringe Competition Law. It is irrelevant for legal purposes whether that form of information is in writing or verbal or whether it's communicated in an informal method; all forms and methods can be caught by Competition Law. It's possible for an employee to infringe Competition Law just by **receiving** commercially sensitive information from a competitor, even if the employee doesn't share any of the Company's sensitive information with that competitor.

Employees must therefore not give to – or receive from – a competitor any non-public, commercially sensitive information, including in relation to pricing, margins, costs, future strategy or any other commercially sensitive issues.

11.4 Abuse of Power in the Market

A company may be considered "dominant" in a market, or to possess a substantial degree of power in it, if it has a strong position in that market. While it is permissible for companies to acquire or hold market power through legitimate competition means, some practices can amount to an abuse of market power in some circumstances.

To help the Company in this respect, employees **must** contact the Legal Department (legal@lcjgroup.com) **before** they negotiate or enter into any of the following arrangements on behalf of the Company:

- Providing "loyalty" discounts or rebates to a Business Partner in return for that supplier or distributor placing all or the majority of its business with the Company;
- Refusing to deal with a particular company or cutting that company out of our potential business dealings;
- Setting prices for a product below its cost value or much higher than its economic value; or
- Engaging in any other behaviour that might be designed to force a competitor out of the market.

Employees should also contact the Legal Department if they suspect that any competitor or Business Partner is harming the Company by engaging in any of these practices.

11.5 Training and External Communications

As mentioned above, the Company provides to relevant staff more detailed training and guidance on this Competition Law policy, as well as a copy of its full Competition Law Compliance Manual. It also communicates the principles of this policy to our Business Partners, principally through the contracts that our Business Partners sign with us. If any employee is asked to assist with arranging for Business Partners to sign any of those contracts, please do so promptly.

11.6 How to Raise Concerns and Seek Guidance about Competition Law

If any employee discovers any activity that could constitute a violation of this policy or Competition Law generally, they must promptly report that activity to that employee's Line Manager or head of Department, as well as to the Legal Department (legal@lcjgroup.com). Employees are encouraged to raise concerns about any instance of possible anti-competitive conduct at the earliest possible stage. As far as possible, all information received from an employee about Competition Law issues will be treated confidentially. The Company will also take the necessary steps to protect the rights of the reporting employee – please see the Company's policy on "whistleblowing" below.

Decisions as to what is acceptable behaviour in Competition Law terms are not always easy. If any employee is in doubt as to whether a potential activity breaches competition law, please **call** the Legal Department to discuss it. If the employee only feels able to report the breach in writing, **please include the following wording at the top of the email or other message** to the Legal Department: "***Privileged and confidential – prepared for the purpose of obtaining legal advice***".

12. WHISTLEBLOWING

Reason For This Policy: The Company is committed to the highest standards of integrity and accountability. In line with that commitment, we strongly encourage employees who encounter any illegal, harmful or unethical activity at the Company to inform us about it, so that we can take prompt, appropriate action in relation to the activity.

12.1 Definitions used in this Whistleblowing Policy

Whistleblower means a person who makes a report or other disclosure, in good faith, about a Reportable Activity (defined below) believed to have occurred at the Company. Whistleblowers may be employees, Business Partners, Customers or a member of the general public. For the most part, this policy discusses Whistleblowers who are employees or those individuals who are otherwise engaged by the Company as part of its workforce, such as independent contractors or freelancers.

Whistleblowing refers to any Whistleblower's report or other alert to the Company, made in good faith, and:

- based on information that reasonably suggests to the Whistleblower that Reportable Activity has occurred at the Company;
- where that information is not otherwise known or readily apparent to the Company; and
- where the Whistleblower may owe a duty to keep such information confidential.

Good faith: Whistleblowers will be deemed to have acted in "good faith" if they:

- have a considered, reasonable basis to believe that their report of the activity is true; and
- make the report without malice or any consideration of a personal benefit to them.

Reportable Activity includes any act of or any omission related to:

- Any criminal offence or failure to comply with legal/regulatory obligations;
- Bribery or other forms of corruption;
- Fraud, malpractice or other possible improprieties relating to financial reporting, internal controls, accounting or audit matters;
- Harassment, Discrimination, Victimisation or Vilification, as defined in this handbook;
- Misuse of the Company's resources, damage to the Company's property or any other conduct that may cause material loss and/or harm to the Company;
- The endangerment of the safety or physical or mental health of any individual;
- Damage to the environment;
- Other breaches of the Company's or Group's policies, Department Policies, codes of conduct, rules, regulations or required procedures, including of any handbook;
- Any other activity a reasonable person would consider illegal, harmful, unethical or alarming.

12.2 Protection of Whistleblowers

The Company will treat fairly and justly any Whistleblower who makes a Whistleblowing complaint in good faith; it will also take the subject-matter of any such complaint seriously.

If the Whistleblowing complaint cannot be confirmed by the Company's investigation, no action will be taken against the Whistleblower(s), unless it is found -- on reasonable grounds -- that the complaint has been raised frivolously, maliciously or for personal gain, in which case the Company may take disciplinary action against the person who so made the report.

The Company will not tolerate any harassment or victimisation of any Whistleblower. Any employee who is found to have harassed or victimised a Whistleblower will face disciplinary action, which may include summary dismissal without compensation by the Company.

12.3 Confidentiality

While Reportable Activities can be reported anonymously, the Company strongly recommends that, during the reporting process, Whistleblowers identify themselves to the Legal or Human Resources Departments or to one of the management members listed below, so that a thorough investigation into the reported matter can be undertaken. Whistleblowers reporting any Reportable Activity must give their name and contact details, so that clarification of the alleged matters or further relevant information can be obtained.

The Company will treat all Whistleblowing reports in a sensitive and confidential manner. Unless required by law or a relevant authority (such as fraud and financial misconduct authorities), the identity of any Whistleblower will not be divulged without the Whistleblower's consent. In a case where identification **is** required by law or a relevant authority, the Company will take all necessary steps to ensure that the Whistleblower suffers no detriment.

12.4 Making a Whistleblowing Report

A Whistleblower should report any Reportable Activities via:

- an email to the Chairman/CEO of the Company or the President of either Lane Crawford Joyce or Imaginex; or
- an email to the Legal Department (legal@lcjgroup.com) or the Human Resources Department; or
- a sealed letter to: LCJG Limited Legal Department, 30/F, One Island South, 2 Heung Yip Road, Wong Chuk Hang, Hong Kong, or the Company's headquarters in Hong Kong at the relevant time.

Please mark any letter "Strictly Private and Confidential – To be opened by addressee only".

A Whistleblower should take care to ensure the accuracy of the information in reporting any Reportable Activity.

12.5 Investigation Procedures for Whistleblower Complaints

It is important to note here that a Whistleblower is a **reporting** party, not an investigator or a finder of fact; the Whistleblower also does not determine the appropriate corrective action that may be warranted in respect of the report.

When the Company receives a Whistleblower's report, it will follow the procedure below:

(i) Within ten working days of receiving a Whistleblowing report, the Company will acknowledge receipt of the report and confirm that the matter will be investigated.

(ii) A member of Executive Management (please see the definition of Executive Management in the Introduction to this Part B of the handbook) who is unconnected with the report's subject-matter will review the Whistleblowing report and, with the assistance of advice from the Legal Department, decide how the investigation should proceed. The Executive Management member will appoint appropriate personnel to conduct the investigation. The objective of that investigation will be to promptly examine information relating to the Whistleblower's allegation, consider the evidence collected about it and draw reasonable conclusions in a fair and impartial manner.

(iii) An investigation report, together with recommendations for improvement or other actions (if appropriate), will be prepared about the allegations made in the Whistleblowing report and submitted to the Chairman/CEO of the Company.

(iv) If there is sufficient evidence to suggest that corruption or a criminal offence exists, the Company will report the matter to the appropriate local authorities for further investigation.

(v) The Whistleblower will be informed of the final results of the investigation wherever legally and reasonably practicable.

12.6 Retention of Records of Whistleblowing

The Company's Legal and Human Resources Departments will securely keep a record of all Whistleblowing reports and any underlying Reportable Activities for a period not exceeding seven years or any other period that may then be specified by Applicable Law. If a reported case leads to an investigation, the person responsible for leading the investigation will ensure that all relevant information relating to the matter is retained (including details of any corrective action that is taken or recommended), and is then promptly sent in an email to legal@lcjgroup.com or the person's usual contact in the Legal Department or an envelope marked "**Strictly Private and Confidential**".

Our Principles: We Protect Our Company's Assets and Reputation

13. COMMUNICATIONS WITH THE MEDIA

Reason For This Policy: The Company and its businesses are topics of interest to the television, print and online press. We need to ensure that when we communicate with any form of media platform we do so accurately, effectively and consistently. For that reason, we ask that all employees comply with this media policy.

13.1 No Media Communication Without Authorisation

Prior Company approval is required for any employee to communicate in any form with the media about or on behalf of the Company or its businesses. No Company employee may offer a public comment on the Company or any of its Business Groups unless that employee has been expressly authorised to do so by the Chairman/CEO or the Group Strategic Communications Department.

13.2 Handling Direct Requests from Media

If any employee receives a request from the media, whether for an interview, statement or comment, and whether on or off the record, the employee must not reply to the media representative substantively. Instead, they should refer the media representative to the Group Strategic Communications Department, who will handle the query on behalf of the Company.

No employee may accept an interview request or other public speaking engagement without receiving approval from the Chairman/CEO or Group Strategic Communications Department.

13.3 Media Training

If any employee is authorised by the Chairman/CEO or the Group Strategic Communications Department to speak with the press or take up any media invitation, the employee will be given training by the Group Strategic Communications Department on the Company's media guidelines. Employees should not take up the speaking engagement or invitation without that training and must comply with the guidelines given to them.

14. USE OF SOCIAL MEDIA AND OTHER PUBLIC COMMUNICATION PLATFORMS

Reason for this policy: We all know that online social media and other public digital platforms are extremely important for effective communication with colleagues, Customers, Business Partners and other third parties. Because social media is still a dynamic and rapidly changing medium, the Company has put in place a policy to protect both itself and its employees in respect of these platforms and to give guidance to its employees when using them.

14.1 Scope of Policy

For the purposes of this policy, **social media** means all online social, sharing and communication platforms, whether they exist now or are developed in the future. This includes all online sharing and communication platforms such as Facebook, WhatsApp, Instagram, Twitter, LinkedIn, Zoom, Skype, Telegram, Line, WeChat/Weixin, YouTube, Microsoft Teams, iMessage and other SMS systems, TikTok/Douyin, Little Red Book/RED/Xiaohongshu and Weibo, among many others.

If the Company's employees don't comply with this Social Media policy's requirements, it could cause the Company significant damage, such as harm to its business reputation, a loss of Customer confidence, decreased competitive advantage, business interruption, litigation, regulatory investigation or financial loss.

As a result, any employee's breach of this policy may lead to disciplinary action against that employee, which could include termination of their employment.

14.2 No Social Media Communications on behalf of the Company without Authorisation

(a) Consistent with the Company's Media Policy in this handbook, the **only** employees who may post on social media **in a manner that suggests they are permitted to represent the Company** are those few staff who have been expressly authorised to speak on behalf of the Company by the Company's Chairman/CEO or the Group Strategic Communications Department.

As a result, unless an employee is expressly authorised to do so as (as set out in the paragraph above), or unless their social media activity falls within one of the exceptions in paragraph (b) below, they should not:

- post content in relation to the Company or its goods, services or Business Partners in a way that suggests the employee represents the Company, or
- identify themselves on social media as an employee of the Company -- this is because other social media users (including potential litigants) may mistake the employee's opinions in those social media forums as those of the Company.

(b) However, Employees **may** forward or re-post on social media any official posts that have been made by the Company or its Business Partners on public platforms, as long as the employee is doing so for the sole purpose of positively promoting or advancing the business of the Company. Additionally, employees may identify themselves as a Company staff member in their professional LinkedIn profiles and posts, provided that this is done in an appropriate, professional way and that the employees ensure that their profile and any content or materials they post are consistent with the professional image they present to customers and colleagues and are in compliance with Company policies.

(c) If, inadvertently or otherwise, any employee does identify themselves on a social media platform as a Company staff member (other than via appropriate LinkedIn use), they must promptly clarify on that platform that any views expressed by them are their own and not those of the Company. Please consider including a short disclaimer to this effect on social media accounts as a matter of course.

(d) The Company may require employees to withdraw or remove any comment or content posted or disclosed on social media that the Company reasonably believes has a negative impact on the Company, its employees or its Business Partners or that contravenes this social media policy, any other Company policy or Applicable Law. Failure to comply with this requirement may in itself result in disciplinary action.

(e) Posts and other communications shared on social media may generate coverage from other media outlets. As required by the Company's Media Policy, employees must immediately refer all media enquiries to the Company's Public Relations Head and Group Strategic Communications for their information and handling.

14.3 Acting Responsibly

As an over-arching principle, when employees are on social media they are expected to act **responsibly and professionally**, within the boundaries of the Company's policies whenever applicable and all Applicable Laws. Employees' social media activity must not damage the Company's standing or act against the Company's best interests.

If employees see harmful comments or insulting posts or communications about the Company or any of its Related Parties on any social media, they should not publicly react to them, but instead refer them to the Group Strategic Communications Department.

14.4 Confidential Information and Social Media

As stated in the Company's Confidential Information policy in this handbook, Employees have a responsibility to protect the Confidential Information of the Company. The prohibition in that policy on employees disclosing Confidential Information of the Company applies to employees' posts or other communications on social media. Disclosure of any aspect of the Company's Confidential Information by way of an employee's activity on social media will result in the same disciplinary action as if the disclosure had occurred in any other way.

14.5 Guidance on Social Media Best Practices

The public image of the Company is often seen through the public representations of its employees. Everything our employees post, publish, disclose or otherwise share on social media can reflect upon the Company. This is an important reason why we expect employees to behave responsibly and professionally when on social media.

The guidelines below set out a few examples of best practices for employees when using different forms of social media. Employees are expected to follow these guidelines and also use their sensible judgment in deciding on the content and conveyance of their communications on social media, particularly when referencing the Company, its businesses, employees or Related Parties.

Employees should:

- Keep in mind that they are legally responsible for any content that they post or publish online in their personal capacity, and that what they publish or post can be public for a long time. The Company will **not** be responsible for employees' inappropriate use of social media and cannot defend them if employees are subject to personal legal liability resulting from that use.

- Ensure the information they post or share on social media is relevant, informed and factually correct. If an employee makes an error in a post, they should admit it promptly.

- Respect the privacy and personal security of others. Before posting or sharing photos or any personal or sensitive data about any person on social media (such as their name, age, contact details, gender, sexual orientation, etc.), they should ensure they have that person's permission to do so.

- When using any social media platforms to conduct or participate in video conferences, meetings, interviews or webinars with any parties related to their employment, such as by using Zoom, Microsoft Teams or Skype, and whether in the Company's workplace or another external location, they should also ensure they enable functionality to prevent the disclosure

of Company information (e.g. while screen-sharing on those platforms). Please do not record the audio or visual content of the meeting unless the other participants in the meeting have consented.

Employees must not:

- Infringe others' rights, including their intellectual property rights and privacy rights.
- Post, proactively access or engage with any material that is inappropriate or illegal.
- Disclose or discuss on social media any non-public Company information, such as unannounced business deals, footage or photographs of Customers, images of Company stockrooms, etc.
- Use the Company's logos, trademarks or other intellectual property unless they have been granted prior permission by the Company to do so. For example, employees should not use the Company name (or abbreviation of it) in their screen name or other social media identifications.

15. CCTV AND IN-STORE PHOTOGRAPHY POLICY

Reason For This Policy: the Company wishes to balance the protection of employees, customers' and other third parties' privacy with (i) a reasonable right for photographs and recordings to be taken in our stores and (ii) the need for appropriate security on Company premises.

15.1 In-Store Photography

The Company has a public-facing, in-store photography policy available on the external websites of its Business Groups that prohibits unauthorised photography and video and/or audio recording for commercial use, private gain, media use or promotional purposes in its retail stores ("**Unauthorised Recording**") and reserves the right to remove offenders of that policy from its premises.

Under that policy, however, reasonably limited photography and video and/or audio recording for non-commercial use **is** permitted in-the stores, subject to the discretion of store management, but store employees have the right to ask Customers or other store attendees to refrain from doing so whenever the person taking the photograph or making the recording is:

- causing concern or a nuisance to an employee, Customer or other person in the store at the time;
- in the reasonable opinion of the relevant employee, causing an obstruction in the store or compromising safety or security there in any way; or
- in the reasonable opinion of the relevant employee, taking Unauthorised Recordings.

If the person taking the photograph or recording in the store refuses to comply with an employee's appropriate request to stop the activity, the employee should promptly inform the store manager and the Company's in-store security staff. Those personnel will immediately review and deal with the situation in an appropriate manner.

There may be circumstances where photographs or recordings are taken that inadvertently capture images of employees which are later posted on social media for Company purposes or by other employees or third parties. The Company will not be responsible for such incidents.

15.2 Closed Circuit Television ("CCTV") Recording

(a) Company's use of CCTV monitoring

The Company uses CCTV to monitor certain, limited areas in its premises ("**Monitored Areas**"), including in its stores, for the primary purpose of maintaining the reasonable security and safety of those areas and the people, assets and other property in them ("**Purpose**"). This monitoring is performed in compliance with Hong Kong's Personal Data (Privacy) Ordinance and its guidelines (the "**Ordinance**").

The Company expressly advises of the CCTV monitoring by placing:

- "CCTV in Operation" notices in the Monitored Areas of its stores and other premises; and
- conspicuous notices at the entrance to each of the premises containing a Monitored Area.

The Company does **not** install CCTV in places where people have a reasonable expectation of privacy, such as in bathrooms or changing areas.

The Company may use CCTV recordings, images, excerpts and data as reasonably necessary in the interests of its business, including assisting in the investigation of any accident or alleged wrongdoing or in compliance with Applicable Law.

(b) Employees' obligations in relation to CCTV generally

CCTV recordings and any still images or other excerpts or data taken from those recordings ("**CCTV Material**") often contain **Personal Data** as defined in the Ordinance – for example, images of individuals' faces and other identifying personal characteristics. Because of this, the Company is required to, and does, have in place strict systems for the accessing, storage, transfer and efficient and timely destruction of CCTV Material, even where certain CCTV Material needs to be retained for a certain period of time because of a relevant safety or security query, investigation or other issue related to the relevant Purpose (a "**Security Issue**").

In brief, the Company's policy is that CCTV Material:

(i) can **only** be accessed via a secure log-in and authentication processes, by a small number of people who have a business-related need to know;

(ii) is only kept for legitimate purposes, including the investigation of complaints, misconduct or security or safety incidents and for legal or insurance purposes; and

(iii) must be securely destroyed once the purpose of the retention of the CCTV Material has been effected or completed.

As a result, **employees who are responsible for monitoring, using or otherwise dealing with CCTV Material** or the CCTV system itself **must** ensure that the legal obligations below are always complied with and the guidance that is separately provided by the Company to such staff ("**CCTV Guidance**") is always followed. If any such employee does not have a copy of the CCTV Guidance, please contact the Legal Department (legal@lcjgroup.com).

(c) Access to and security of CCTV Material

Security measures must be effected to prevent unauthorised access to the CCTV system and CCTV Material. All CCTV Material should be kept in safe custody for the relevant period of time for which it is permitted to be retained, as follows:

(i) The servers, hard drives or any devices storing digital CCTV Material must be securely protected from unauthorised access, such as by way of an encryption function.

(ii) A log-in and password must be used for access to and storage of digital CCTV Material, which may only be made available to authorised users responsible for the CCTV system who have been duly approved in writing ("**Authorised Internal Users**") and noted in the Company's log of CCTV Authorised Internal Users.

(iii) Hard copy CCTV Material must be locked in a secure location, available only to Authorised Internal Users.

(iv) Access to any locations where CCTV Material is viewed, stored or handled must be secured and restricted to Authorised Internal Users only, unless the prior written permission of the Legal Department is obtained.

(v) Authorised Internal Users are only permitted to view or otherwise use the CCTV Material when they receive a legitimate report of a Security Issue for which the CCTV Material may be relevant.

(vi) If an employee or other person who is not ordinarily an Authorised Internal User requests to view, access or otherwise use our CCTV Material, please do **not** handle any such request themselves. Instead, promptly forward the request to the Legal Department, who will decide whether to grant the requested permission. Please note: if the Legal Department grants this permission, the permission will only apply to the particular requested use of the particular CCTV Material and will be subject to the requirements of Applicable Law.

(vii) Only an Authorised Internal User may operate the playback of CCTV Material, regardless of who is viewing that CCTV Material.

(viii) Any viewing, access or other use of CCTV Material by a person who is not ordinarily an Authorised Internal User **must be documented** in the Company's CCTV log by the actual Authorised Internal User handling the matter, in accordance with the Company's CCTV Guidance.

(ix) Authorised Internal Users and other permitted recipients (as above) must **only** use the Personal Data in the CCTV Material for the relevant Purpose or a directly related purpose, unless:

- the person who is the subject of that Personal Data (e.g. each person in the relevant CCTV footage) gives **written** voluntary consent; or
- the Legal Department advises in writing that an applicable exemption under the Ordinance applies.

(d) Transfer of CCTV Material

Because CCTV Material is usually confidential and may include sensitive personal data, any disclosure or transfer of it ("**transfer**") **must** comply with the following requirements:

(i) The CCTV Material may only be transferred as a result of a reported Security Issue;

(ii) **Unless** the permission of the Legal Department has been received in respect of the particular transfer, the CCTV Material **must not be transferred to any person or organisation other than** the Legal Department or another current Authorised Internal User who is assisting with the Security Issue. This restriction applies regardless of the form in which the CCTV Material is to be transferred – i.e. whether in digital format (e.g.

via email, digital messaging service, mobile telephone or other digital device) or in hard copy. Accordingly, if an employee or other person who is not ordinarily an Authorised Internal User requests a copy of any CCTV Material, **the request must be sent to the Legal Department** for review and decision.

(iii) No person (not even an Authorised Internal User) may transfer any CCTV Material through **social media or text messaging services**, including via WhatsApp, WeChat, or via non-company email accounts such as Google Mail.

(iv) Any copy of the CCTV Material to be digitally transferred **must be encrypted** and password-protected before the transfer, and the password for it must be separately communicated to the recipient.

(e) Enquiries about CCTV Material by police/law enforcement or regulatory agencies

(i) If an officer of a law enforcement agency (e.g. the Police) or a regulatory agency (e.g. the Labour Department) **calls or writes** to request or demand access to our CCTV Material, the Legal Department must be informed immediately. The Legal Department will then decide whether the Company should comply with the request or demand.

(ii) If an officer of a law enforcement or regulatory agency **visits our premises** to request or demand access to our CCTV Material, please ask them to complete and sign the following form **before** addressing their request:

I, [full name of officer] (Officer/Police Identity/Badge No._____), request to view CCTV footage of [name and address of the store or Company premises] between [time] and [time] on [date], for the purpose of the prevention or detection of crime as permitted by the Personal Data (Privacy) Ordinance.

Signature of Officer: _____
Name of Officer: _____
Date: _____

Please then inform the Legal Department of the request or demand **as soon as practicable**.

If the officer or agency refuses to complete and sign the above form, please contact the Legal Department (legal@lcjgroup.com) or your usual Company lawyer **immediately**.

(f) Destruction of CCTV Material

(i) The Company's regular destruction process for the timely and secure destruction of CCTV Material that is **not** required in respect of any Security Issue must be effected fully and on time.

(ii) CCTV Material that is needed to be retained as a result of a Security Issue should be removed from the above regular destruction process and stored **securely** while the Security Issue is looked into.

(iii) Once a reported Security Issue is resolved, closed or is no long active, the CCTV Material relating to it must be securely destroyed as soon as practicable.

(iv) When destroying CCTV Material, the following methods should be used:

- if the CCTV Material is held in hard copy form: by first shredding and then securely disposing of it; and

- if the CCTV Material is held in electronic form, by permanently erasing it from our systems.

(v) In either case, at that time, all Authorised Internal Users:

- who hold a copy of such CCTV Material (whether in hard copy of electronic form) must also securely and permanently destroy that copy; and

- who transferred a copy of such CCTV Material to another person (whether in hard copy of electronic form) must require that person, in writing, to securely and permanently destroy that copy.

(g) Personal Data requests

If a person whose image or other personal information has been captured by our CCTV system asks us for a copy of the relevant CCTV Material, please forward the request **as soon as possible** to the Legal Department (legal@lcjgroup.com).

(h) Misuse and compliance

(i) If any employee sees any misuse of the CCTV system or CCTV Material, they must immediately report it to the Legal Department (legal@lcjgroup.com).

(ii) The head of the relevant Department or Business Group responsible for the CCTV system must ensure that an annual compliance audit is carried out in respect of the CCTV system, CCTV Material and the above required protective measures, so as to assess the effectiveness of the security of the CCTV Material and system and the compliant implementation of the above required measures. Any issues that are found in relation to the implementation of the above required measures must be promptly reported to the Legal Department and remedied.

16. USE OF COMPANY'S ELECTRONIC SYSTEMS & CONTENT

Please note: This Use of Company's Electronic Systems & Content policy is contractual in its effect and applies **in addition to** any obligations under an employee's employment contract or any separate agreement.

Reason For This Policy: Information technology and other electronic and communication systems are a powerful tool for organisations and their staff. Advances in information technology and the increasing number of technology systems via which information can be communicated and otherwise handled have created situations that may not have been adequately addressed in the past. The aim of this Electronic Systems and Content policy is to ensure that the technology resources of the Company are used properly, legally and efficiently.

Subject to some exceptions expressly set out below, the Company's Electronic Systems and Content should only be used for the Company's business purposes. They should never be used for illegal purposes or for activities that breach any provision of this handbook.

16.1 What are the Company's Electronic Systems?

The "**Electronic Systems**" include the Company's:

- servers, networks, intranet, email and other communication systems;
- audio and/or video recording mechanisms;
- data collection and processing systems;
- Internet access applications, machine-learning platforms and other licensed electronic applications (including mobile versions);
- software and technology infrastructure, as well as technological devices used for the Company's business purposes, such as computers, mobile telephones and tablets, portable digital storage media and other electronic hardware.

Except where expressly stated in this handbook, this Electronic Systems Policy also applies to mobile telephones, tablets or personal computers that are not provided by the Company but are nonetheless used by employees for Company business purposes ("**Personal Devices**").

Please note that employees:

- should **not** use their personal email accounts to conduct or otherwise participate in work activities or for other Company business purposes;
- should ensure that any electronic messaging accounts (such as WhatsApp, WeChat, etc.) they use for work-related purposes ("**Messaging Content**") are backed up regularly, effectively and securely; and
- should use their Company email accounts for work purposes **only**.

16.2 Use of the Company's Electronic Systems

The Company's Electronic Systems, including the access provided by some of those systems to the Internet and communication platforms, should be used principally for the conduct of Company business. Occasional personal access is acceptable, but must be kept to a reasonable level and must comply with local laws. Employees must exercise good judgment when using the Company's Electronic Systems for their occasional personal use and comply with all Company policies.

In particular, employees must not use the Company's Electronic Systems for any purpose or objective that:

- is illegal, unethical or in breach of any policy, rule, regulation or handbook, including to defame or infringe any person's rights;
- involves the receipt, viewing, downloading, sending or posting of any abusive, offensive, disrespectful or discriminatory messages or content, including sexual content;
- is for the personal profit-making of an employee or third party;
- is to the detriment of the Company or its Business Partners; or

seeks to compromise the security of the Company's Electronic Systems or any information contained in or on any of them.

Employees' use of any commercial software (including applications) provided to them by the Company is strictly governed by the Company's licence agreements for the respective software. These licence agreements authorise the use of the software under clearly defined conditions and operating environments only. Employees must not make any copy of the Company's licensed software, manuals or other documents; such acts may breach applicable intellectual property laws.

Employees must not download, install or use any illegal, unlicensed or unauthorised software on or via the Company's Electronic Systems, including any freeware or shareware that has not been authorised by the Company's Tech/IT Department, regardless of the source or form of it. All installation, re-installation, upgrade and/or transfer of Company-supplied software on or between devices or hardware used for Company purposes, regardless of whether they are supplied by the Company or Personal Devices, may only be carried out by employees from the Company's Tech/IT Department.

The Company may, at any time it deems necessary and without any notification, inspect any software, files, content or data stored in or on the Electronic Systems and remove any unauthorised, unlicensed or illegal software or content without prior notice to employees. It may also use any inspected materials for the purposes of investigations into possible wrongdoing in relation to the Company or its businesses, policies or contractual or legal obligations.

16.3 Ownership of Electronic Content

All electronic materials, files, information, communications and other electronic content created, transmitted, received or stored via the Company's Electronic Systems ("**Electronic Content**") are the property of the Company. This includes work-related Messaging Content.

Employees must treat the Electronic Content with the highest degree of care and diligence. Employees must not distribute, alter, remove, destroy or tamper with any Electronic Content recklessly or with deliberate or malicious intention, or in any way that results in detriment to the Company's interests. The Company's Confidential Information policy in this handbook applies to all confidential Electronic Content.

Any mishandling of any Electronic Content will be taken extremely seriously by the Company and may also incur legal liability. The Company reserves the right to take appropriate action, including possible legal action, against any employee in breach of this Electronic Systems policy in order to recover or secure its Electronic Content and/or to obtain damages in accordance with Applicable Law.

Employees must not download any digital content or online materials on or via the Electronic Systems that are illegal is illegal, unethical, unauthorised by the Company or in breach of any part of this handbook. Downloading such materials increases the risk of introducing viruses into the Company's Electronic Systems and may also contravene intellectual property and/or licensing laws.

Any digital information or content sourced from the Internet, including from social media platforms, must be thoroughly validated for authenticity, relevance and rights of use before being used for any Company business purposes or decision-making.

16.4 Security of the Company's Electronic Systems and Content

Employees must ensure that their passwords to their Personal Devices and the Company's Electronic Systems are difficult to guess, kept safe, not given to anyone other than to Executive Management (please see the definition of Executive Management in the Introduction to this Part B of the handbook) or the Tech/IT Department (if requested) and changed regularly, preferably at least once every three months. If the Company requires any employees to disclose a password related to Company information or purposes due to urgent operational needs, those employees should promptly comply and then change those passwords immediately after that need has passed.

Employees must not log in to any of the Electronic Systems as another employee without the express approval of that other employee. Even with that approval, they may do so only for legitimate Company purposes.

The Company reserves the right to modify any employee's password(s) to the Electronic Systems in order to gain access to any information within those Electronic Systems.

Employees should ensure that they back up their Personal Devices to an established and reputable cloud server, where their data is encrypted and securely stored.

The Company may, if it believes necessary for an employee's job performance, authorise the employee to log in in to the Company's Electronic Systems from premises outside its offices, whether via the use of special passwords or other Company-supplied security functionality. These employees must exercise utmost care and discretion in their remote use of the Electronic Systems and not disclose their passwords or any other required security measures for such remote use to any unauthorised party. The Company may terminate any remote access without prior notice.

16.5 Preservation, Monitoring and Review of the Company's Electronic Systems and Content

To protect its business interests, the Company reserves the right to back up, record and/or monitor any of the Electronic Systems and to inspect, process, copy, store and use any of the Electronic Content (including transactions, emails, work-related Messaging Content, other messages, social media posts, log-ins, recordings and information concerning the use of Electronic Systems), at any time and without prior notice, and in each case to the maximum extent permitted by Applicable Law and Company policies.

The Company has installed a system whereby all incoming and outgoing customer service calls are recorded and all email messages sent through the Company's server are recorded and logged. A similar type of protocol may be implemented for future messaging, online or voice systems licensed by the Company for staff business use. Please remember that the content of any messages sent or received by employees using the Company's Electronic Systems constitutes Electronic Content under this policy. As such, it may, to the maximum extent permitted by Applicable Law and regulations and without prior notice to any employee, be recorded, inspected, disclosed and used by the Company in its conduct of legitimate Company operations and processes. By indicating their acceptance of this handbook, employees expressly consent to these practices.

CCTV cameras with recording facilities have been and will continue to be deployed in Company locations as are deemed necessary by the Company. Employees expressly consent to this. It is the intention of the Company that, by the use of such facilities, the Company can better provide a safe working environment to all employees, prevent and protect employees against crime, improve performance management and review working practices. The Company's CCTV policy is also set in this handbook.

16.6 No Expectation of Privacy

Employees understand and agree that they have **no expectation of privacy** in relation to the use by them of the Company's Electronic Systems and Electronic Content (including work-related Messaging Content), including the access to and use of the Electronic Systems and Electronic Content, whether via Personal Devices or otherwise. Employees also understand and agree that the Company reserves the right to access, monitor, extract, transfer and review employees' communications in relation to the Company's business, operations and assets, as well as their use of the Company's Electronic Systems and their use of the Internet via those systems at any time (collectively, the "**Monitoring & Review Right**").

The circumstances in which the Company may use this Monitoring & Review Right may include:

- to facilitate the efficient provision of products and services to Customers;
- to ensure that the Company is able to refer to the full background to (i) deals that are proposed, negotiated or concluded with its vendors or other third parties and (ii) other operations or business of the Company;
- during internal or external investigations or audits or to comply with governmental or regulatory inquiries or requests;
- where a potential breach of Company policy or Applicable Law is suspected or investigated or to check compliance in those respects;
- to ensure that the Company complies with its contractual and legal obligations;
- to maintain a stable and secure Electronic Systems service environment for communications;
- to protect its premises, its workforce and any sensitive or confidential information belonging to the Company;
- to monitor performance at work, ensure proper utilisation of the Company's resources and prevent misuse of the Electronic Systems used for the Company's business purposes; and
- otherwise to protect the legitimate interests of the Company,

in each case to the maximum extent permitted by Applicable Law.

This Monitoring & Review Right extends to the monitoring, accessing, collection, processing, reviewing, use and deletion of any and all outgoing and incoming emails and other messages or data related to the Company's business that are stored on any Personal Devices and any logs or copies of them, to the extent permitted by Applicable Law. Employees are advised **not** to use the Company's Electronic Systems for any matter intended to be kept private or confidential. Employees must cooperate with the Company to enable it to exercise the Monitoring & Review Right, including providing any passwords, PIN numbers or other security requirements to access devices or relevant applications.

Information identified and collected during the above exercises may be used and stored for as long as necessary for the purpose of the above exercises, including for:

- the duration of the investigations; and
- the period necessary to defend and claim any right of the Company; and
- for the term of any potential dispute in relation to it,

and otherwise in accordance with Applicable Laws.

Information identified and collected during the above exercises can be disclosed to third parties when required for the above investigations, right or dispute or otherwise in accordance with Applicable Laws.

In any event, the Company may retain all information concerning any employee's misuse of the Electronic Systems for at least seven years after the end of that employee's employment with the Company, in order to protect and defend the Company's rights in this regard, although there may be extensions of this time period for this purpose on a case-by-case basis if the circumstances warrant

at the relevant time. However, information about that employee's use of the Internet via the Company's Electronic Systems (i.e. the origin and destination information stored in the Electronic Systems' proxy server logs will only be retained for no longer than 6 months from the date of collection of it.

16.7 Network Management

The Tech/IT Department is responsible for planning, implementing and managing the Company's broadband network, including wireless connections to it. The following technologies cannot be implemented in the Company without the consent of the Tech/IT Department: routers, switches, hubs, wireless access points and other networking technologies.

16.8 Bring Your Own Device ("BYOD") policy

(a) Purpose of the BYOD policy

Subject always to the Company's policies, employees may use their Personal Devices for work-related purposes, solely to connect with the Company's network and to access authorised parts of the Company's Electronic Systems for work-related purposes, including accessing and using the Electronic Content and potentially accessing non-public, sensitive, confidential and/or proprietary information of the Company for work-related purposes (the "**BYOD Use**"). This BYOD policy is part of the Company's Electronic Systems and Content policy and is intended to protect the security and integrity of the Company's Electronic Systems and Electronic Materials from risks associated with devices not owned by the Company that connect to its Electronic Systems and use, transmit or store its Electronic Content.

Employees should feel free to ask the Tech/IT Department for their detailed BYOD guidelines, which will assist staff to comply with the policy.

Limited exceptions to this BYOD policy may occur due to variations in devices and platforms. Please submit any request for such an exception to the Tech/IT Department.

(b) Acceptable BYOD use

Employees must use their relevant Personal Device(s) for work purposes in a legal, ethical and professional manner.

All BYOD Use must comply with the Company's policies, including the Confidentiality, Intellectual Property and Use of Social Media Use policies in in this handbook, as well as the remainder of this Electronic Systems & Content policy.

In order for a Personal Device to be permitted to be used for work-related purposes, it must:

- have the ability to connect to the company's secure Wi-Fi network;
- support encryption for data storage and transmission;
- be compatible with the company's chosen Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) or Enterprise Application Management (MAM) solution; and
- have the latest operating system and security updates installed.

(c) Security

In order to protect the Company's Electronic Systems and Electronic Content and to protect personal data privacy:

- Each Personal Device must be securely protected throughout the period of time during which the employee uses the Personal Device to access and/or use the Electronic Systems and/or Electronic Content, whether by way of strong passwords, biometric authentication or other security measures expressly approved by the Tech/IT Department;

- Employees must not store any of the Company's Electronic Content on any unapproved mobile applications on their Personal Devices;

- Employees may not copy the Company's Electronic Content to any other device or storage media not owned by the Company.

- Employees must not store sensitive or confidential Electronic Content of the Company on their personal devices without proper encryption and authorisation.

- Employees must only access the Company's Electronic Content and Electronic Systems through secure connections, such as the Company's VPN or secure Wi-Fi.

- Employees must keep their Personal Devices updated with the latest security patches and antivirus software.

- Employees must not intentionally download pirated software onto their Personal Devices or use their Personal Devices to access, store or transmit any illegal content or engage in activities that violate Company policies.

- In the event of a lost or stolen Personal Device, employees must allow the Tech/IT Department to remotely wipe Company data from the device.

- Employees are responsible for ensuring the security and integrity of their own Personal Devices and personally-managed systems.

(d) Removal of work-related mobile applications

By accepting this handbook, employees expressly consent to the Tech/IT Department accessing on and/or removing from their Personal Devices all work-related mobile applications, all the Company's Electronic Content and any other access right of the employee to the Company's Electronic Systems in the following circumstances:

- upon termination of the employee's employment with the Company for whatever reason (or, where applicable/earlier, upon commencement of any suspension, garden leave or unperformed termination notice period);

- if the Tech/IT Department detects a data or policy breach or a virus or similar threat to the security of the Company's Electronic Systems or Electronic Content; or

- in any other situation that the Company deems appropriate.

In the event that the Tech/IT Department must effect the removal actions set out above, it is the employee's responsibility to take precautions to protect their personal data and applications on the Personal Device, such as backing up their personal data to another device or storage media. The Company will not be responsible for the loss or damage of personal applications or data resulting from the BYOD Use or the removal actions described above.

(e) Loss, unauthorised access and costs

Employees must immediately report the theft or other loss of their Personal Device to both the Company and the employee's mobile network provider. Employees should activate any "remote data-wiping" functionality offered by the operation system of their Personal Device and utilise that functionality if the Personal Device is stolen or otherwise lost.

If an employee suspects that unauthorised access to Company data has taken place via an employee's Personal Device, the employee must immediately report the incident to the Company and provide all relevant details.
Each employee is personally liable for all costs associated with that employee's Personal Device. Each employee assumes full liability for all risks associated with the BYOD use, including the partial or complete loss of Company data (including the Electronic Content) or personal data due to any operating system crash, programming errors, bugs, viruses, malware and/or other software or hardware failures that render the Personal Device partially or wholly unusable.

16.9 Notice of Data Protection Compliance

The Company has taken into account applicable data protection legislation when preparing this Electronic Systems & Content policy. To the best of its knowledge, after due investigation, the Company believes that the collection of information and data in the course of all monitoring and data collection by the Company complies with Applicable Law. The Company performs the monitoring and collection for the purpose of addressing inherent business risks, unauthorised and unlawful activities and such other activities as permitted by Applicable Law. Storage and access to all information collected under the Monitoring and Review Right will be effected in accordance with the requirements of Applicable Law.

17. "DAWN RAIDS" (SEARCHES OF COMPANY PREMISES & DEMANDS FOR COMPANY INFORMATION OR PROPERTY) AND BUSINESS SCAMS

Reason for this Policy: The Company fully intends to comply with all legitimate, authorised searches of its premises and all legitimate, authorised demands for its information, provided that the searches and demands are effected in accordance with Applicable Law. However, the Company will also take measures to review the legal basis of any such search or demand, so that it may endeavour to protect its employees, confidential and legally privileged information, intellectual property rights and the personal data of staff and third parties that it holds. This policy summarises those measures, for the information of staff.

17.1 What is a Dawn Raid?

In many countries, including Hong Kong, the government's competition law and fraud agencies, certain other regulatory authorities and law enforcement agencies such as the Police have powers to conduct unscheduled, on-the-spot investigations at any company's premises. These unscheduled investigations are often called "Dawn Raids". As a result, an agency, regulatory authority or Police investigators (each an "**Investigator**") may arrive at the Company, **unannounced and at any time**, to demand, search for, copy and take away documentation and other items and may question Company representatives for information. Employees have the right to deny any such entry, access or search request (if it is safe to do so) without having first been presented with a search warrant (or similar

authorization document) allowing them to enter the Company's premises and/or search and/or copy files) by such officials.

If any employee sees or learns of a Dawn Raid taking place at the Company's premises, they must immediately call the Legal Department.

17.2 What to do in a Dawn Raid

The Company separately provides certain frontline staff at our premises with full guidelines concerning Dawn Raids, as those staff are the people most likely to encounter Dawn Raid investigators at Company premises. If any employee believes themselves to be such a frontline staff member for this purpose and has not received these guidelines, please contact the Legal Department (legal@lcjgroup.com).

The following is therefore a **summary only** of the key points to keep in mind in the event of a Dawn Raid in our workplace:

If an employee encounters Investigators conducting, or about to conduct, a Dawn Raid at the Company's premises:

- As mentioned above, contact the Legal Department **immediately**.
- Be calm and polite to the Investigators at all times, but do not approach them or engage them in conversation unless asked by them to do so.
- If the employee is asked to talk to the Investigators, ensure that a member of the Legal Department or our external legal counsel is present for that conversation. In that situation, politely explain to the Investigators that staff must decline to talk to them until legal counsel arrives.
- Do not provide false or misleading information to the Investigators, conceal or destroy documents or alert any third party to the fact of the investigation.
- Do not give any documents or information to the Investigators without prior approval from the Legal Department or the Company's external legal counsel– **unless** it is unsafe to refuse a demand by them.
- To the extent possible, ensure that while the Investigators are on the Company's premises, they are accompanied at all times by appropriate Company employee(s), such as a member of the Legal Department or executive management, or the Company's external legal counsel.
- Do not speculate on the reason for the investigation with any other person, either in-person or via any other medium.
- Refer any enquiry from the media about the Investigators or the investigation to Group Strategic Communications. Employees must **not** comment on any such enquiry themselves.
- Employees should seek immediate advice from the Legal Department if at any time they are uncertain of their rights and responsibilities during a Dawn Raid.

17.3 Business Scams and Other Fraudulent Demands

Other people who may appear to be an authority figure, such as those who represent themselves as being a Company executive, a Hong Kong or PRC police officer or a government representative, may actually be fraudulent third parties trying to conduct a scam against the Company. These people often request or demand that an employee (i) provide the person (i.e. the scammer) with Company information or (ii) perform an activity in relation to Company resources, such as paying out Company funds or approving such a payment.

(a) Calls from possible scammers

If any person unknown to an employee calls the employee with such a demand, the employee should ask for the person's full name, title and identification number (such as the Officer Identification Number, in respect of Police), the person's agency/authority name, telephone number and supervisor email address. If the called gives the employee any of this information, the employee should write it down, then hang up and call either the head of the Corporate Finance Department (CorpFinancePolicies@lcjgroup.com), the head of the Human Resources Department or any member of the Legal Department, asking them to investigate the demand.

(b) Messages from possibly scammers

If an employee is instead contacted by such a person by email or in another written form, the employee should send the message to the head of their respective Finance or Human Resources Departments or any member of the Legal Department, and ask them to advise the employee if the message is authentic.

(c) Business Email Compromise fraud

A particularly dangerous and common type of scam against companies is what is known as CEO fraud or Business Email Compromise ("**BEC**") fraud. This usually involves a hacker gaining access or other visibility over a Company executive's contacts, emails and/or movements, then pretending to be that executive via an email or other message while the real executive is on holiday, on a flight or otherwise relatively out of touch. The message usually purports to be a legitimate request from the executive to send a sum of money to a third party bank account.

Some of these messages are **extremely convincing** – they can look like they come from an LCJG email address, the sender may know a number of employees' and other executives' names and our payment processes, and the messages may refer to the need to make a payment to an actual vendor of the Company or for an actual deal that we're currently involved in.

To help recognise and avoid BEC fraud attempts, employees should make sure they:

(i) Always check payment instruction emails closely, particularly ones that say they are urgent, to ensure they are from the **actual email address** of the relevant company executive(s), and not just from a name very similar to the executive's name or the company's email domain.

For example, the email domain might look like it's @lcjgroup.com, but is actually @lcjg.com, @lcjgroup.com.hk.com or @lcjg.com.cn. Often a person's brain will just skip over such a small error in a name;

(ii) Be wary of emails that seem to be sent from familiar people, but from a different email domain (e.g. @gmail.com or @mac.com instead of their company email address), particularly when the apparent sender justifies this use of a different email domain by saying something like "I'm working from home today" or "this is my personal email account";

(iii) Ask themselves if they were expecting the payment request;

(iv) Be similarly wary of messages that seem to come from vendors or other business partners, stating that their bank account number has changed and asking that a (legitimate/scheduled) payment be paid into the "new" bank account promptly. This type of message is often from scammers who have hacked into the relevant vendor's systems;

(v) Confirm any such request -- **by phone** -- with the person who's apparently giving the instruction, such as the apparent Company executive. Also confirm with the apparent vendor/payee – again **by phone --** that as to whether the payment should be sent to the bank account number set out in the message. **Do not do any of this via email or another messaging platform**.

When phoning, employees should make sure that the phone number used is one they already have for the executive or payee; they should not use one from the potentially fraudulent message;

(vi) Keep in mind that gmail.com, outlook.com and the like aren't as secure as our own email domain. As a Company employee, don't use these personal email services for sending work emails. And, of course, **don't send any confidential information of the Company** over them.

The Corporate Finance Department (CorpFinancePolicies@lcjgroup.com) will send out further guidelines on BEC fraud.

18. THIRD PARTY RIGHTS UNDER EMPLOYMENT CONTRACTS

Reason For This Policy: The Company's employment contracts are written for the benefit of, and enforcement by, solely the parties to that contract. Under Applicable Law, the Company can opt out of any provision to the contrary in the Contracts (Rights of Third Parties) Ordinance in Hong Kong. This is the intention and effect of this policy.

A person who is not a party to a contract of employment between the Company and an employee shall not have any rights under Hong Kong's Contracts (Rights of Third Parties) Ordinance to enforce or enjoy the benefit of any term of this handbook.

In addition, despite that Ordinance, employees have no right to enforce this handbook against any person or company other than a party to the employee's contract of employment.

ACCEPTANCE OF THE HANDBOOK

We thank all staff for reading this handbook. If there are any questions about it, please contact the Human Resources Department or the Legal Department.

Please acknowledge acceptance of this handbook via this password-protected link: https://portal.lcjgroup.com/staff_handbook, or via any updated link that the Company provides to employees in the future.

We encourage staff to regularly refer to this handbook (as amended from time to time) for the Company policies that relate to their employment. The Company will keep employees informed of any update or change to the handbook, or other important staff information, through emails, intranet notices or other announcement methods. In the meantime, employees should feel free to contact the Human Resources Department to discuss any part of the handbook.