Company Name

Drugs Policy

Last updated date:

Introduction

[***Insert Company name***] are responsible employers and we take our obligations to our employees very seriously. This is why we have set out this policy to help us ensure the health, safety and welfare of our employees and to help us comply with our legal duties.

- Section 2(2)(e) of the Health and Safety at Work Act 1974 places a duty on employers to provide a safe and healthy working environment.
- It is an offence to supply, produce, offer to supply or produce controlled drugs.
- The Misuse of Drugs Act 1971 makes it an offence for the occupier of premises to permit knowingly the production or supply of any controlled drugs or allow the smoking of cannabis or opium on those premises.
- It is also an offence to aid or abet any of these offences.

This policy covers all employees, **[**consultants**],** contractors, volunteers and agency workers.

All managers have a specific responsibility to operate within the boundaries of this policy, to ensure that all staff understand the standards of behaviour expected of them and to take action when behaviour falls below its requirements.

Any reference in this Policy to a non-prescription drug refers only to controlled or illegal substances and does not refer to medicines, supplements and similar substances that are legally and commercially available in the United Kingdom.

Aims of the Policy

This Policy aims to:

- Comply with the Company's legal obligations to provide a safe and healthy working environment for all staff;
- Comply with all of the requirements imposed by law;
- Raise awareness of the effects of drug misuse and its likely symptoms;
- Ensure that employees are aware of their responsibilities regarding drug misuse and related problems; and
- Ensure that employees who have a drug-related problem affecting their work are dealt with sympathetically, fairly and consistently.

Health and Safety

Misuse of drugs can lead to reduced levels of attendance, reduced efficiency and performance, along with impaired judgement and decision-making. Employees should be aware that anyone under the influence of controlled drugs is a risk to everyone around them and should be alert to possible signs of

drugs abuse. Such indicators commonly include:

- Sudden changes in behaviour;
- Confusion;
- Irritability;
- Fluctuations in mood and energy;
- Impairment of performance; and
- Increase in short term sickness absence.

If employees notice a colleague displaying any or all of these symptoms, employees should encourage them seek assistance through their manager **[*insert name and Job Title*]** If they will not seek help themselves, employees should draw the matter to the attention of their manager. Employees should not, under any circumstances, discuss their concerns with any other colleagues.

If employees are prescribed medication, they must seek advice from their GP about the effect on their ability to carry out their job and whether duties should be modified. If so, employees should advise **[*insert name and Job Title*]** immediately.

Searches

The Company reserves the right to conduct searches for drugs on Company premises including searches of [***bags, lockers, cabinets***].

Prohibition

- Employees are expected to arrive at work fit to carry out their job and to be able to perform their duties safely without limitations due to the use or after-effects of drugs. The use of drugs also includes the use of substances formerly known as “legal highs” or psychoactive drugs, which are legal substances which have the effect of illegal drugs.
- No non-prescription drugs can be consumed in, or brought onto, company premises, land or vehicles at any time by any person irrespective of their status in, or business with, the Company.
- The prohibition of non-prescription drugs extends to all activities carried out by staff whilst they are at work. These activities include, but are not restricted to, driving on company business, when on call or standby duties or when on trips for company business, training or social events.

Disciplinary Action

A breach of these rules will be defined as gross misconduct and it is likely that the employee in question will face summary dismissal. If, however, an employee agrees to undertake appropriate treatment and/or rehabilitation for an acknowledged drug-related problem, the Company may decide to suspend any ongoing disciplinary action for related misconduct or poor performance pending the outcome of the treatment.

Principles

- All information relating to an employee’s health including, but not limited to, matters involving drugs, will be collected, held, and processed in accordance with the Company’s [Employee] Data Protection Policy.

- If an employee is diagnosed as having a drug-related problem the Company will treat it as a health matter. This does not however excuse the employee from any of the disciplinary matters that may fall within the scope of the Company disciplinary policy.
- Drug-related problems may develop for a variety of reasons and over a long period of time. All drug-related issues will be dealt with, as far as possible, in a constructive and sympathetic manner. The person responsible for all such issues in the Company is **[*insert name and Job Title*]** who will also provide employees with the details of where to seek further information and help.
- All requests for help will be treated in the strictest confidence and all information gathered as a result will be held in accordance with the Company's **[**Employee**]** Data Protection Policy. However, it must be recognised that, in supporting staff, some degree of information-sharing is likely to be necessary.
- The Company reserves the right to give affected employees lighter duties at the same rate of pay or require them to take paid leave if it is deemed appropriate.
- Following effective treatment and in the absence of any disciplinary action the Company will endeavour to return an affected employee to the same role previously fulfilled by the employee **[**and, where this is not possible. to a suitable alternative**]**.
- In the event that an employee following successful treatment for a drug related problem suffers a relapse the Company **[**will not make**] [**is under no obligation to make**]** provision for any further treatment and the employee in question **[**will**] [**may**]** face summary dismissal. If it is considered that the working environment or culture is the cause or a contributor to a drug related problem, the Company will take all reasonably practicable steps to ensure a reduction of such problems.

This policy has been approved and authorised by:

Name:

Position:

Date:

Signature:

Company Name

Alcohol Policy

Last updated date:

Introduction

[***Insert Company name***] are responsible employers and we take our obligations to our employees very seriously. This is why we have set out this policy to help us ensure the health, safety and welfare of our employees and to help us comply with our legal duties. Employees who develop alcohol related problems cause harm to themselves, to others and impair their performance.

The Health and Safety at Work Act 1974 places a duty on employers to provide a safe and healthy working environment, and to ensure the health, safety and welfare at work of their employees as well as any visitors or contractors on the premises.

Aims of the Policy

This policy aims to:

- Promote awareness of alcohol related problems and addiction;
- Encourage a sensible approach to drinking alcohol;
- Ensure that the Company complies with its legal obligations;
- Indicate restrictions on drinking alcohol at work;
- Protect Employees from the dangers of alcohol abuse; and
- Support Employees with an alcohol related problem.

Health and Safety

In a social environment the consumption of alcohol in moderation is an accepted part of life. In the workplace however it can impair performance, result in inappropriate behaviour, and can place both the individual and those around them in danger, as well as affect health.

In the workplace alcohol abuse can take two different forms:

- Occasional inappropriate drinking; and
- Consistently inappropriate drinking.

Problems arising from the first category are more likely to be cases of misconduct whilst the second will be more likely to involve long term health and performance issues. In either case the health of the individual employee will be affected and quite possibly the health and safety of those around them.

While it will be clear if an individual is drunk at work, the symptoms of larger scale systematic alcohol abuse may be less obvious. Symptoms of alcohol abuse may include:

- Frequent absences on Mondays and Fridays;
- Unusually high rates of absenteeism;
- Unkempt appearance/Lack of hygiene;
- Spasmodic work patterns and lower productivity; or
- Poor relations with others.

Restrictions on Drinking Alcohol at Work

- Unless it is formally approved by [***insert name and job title***] employees may not consume alcohol during normal working hours nor should they be incapable of work through the consumption of alcohol.
- colleagues or visitors is put at risk.
- Alcohol must not be consumed in excess [or in sufficient quantities to impinge on the exercise of any individual's duties] when on Company business outside normal working hours, for example when involved in functions or in providing hospitality.
- Employees are not obliged to work with anyone they consider to be incapable through the consumption of alcohol and should immediately report the matter to [***insert name and job title***].
- Employees who are incapable of working through the consumption of alcohol should be immediately removed from duty and the matter reported to [***insert name and job title***].
- Employees will be held to be contributory negligent in the event that whilst on Company business they cause an accident or damages to anyone or anything, and that the incident occurred due to the Employee's consumption of alcohol.

Disciplinary Action

Employees who are unfit or otherwise incapable for work through the consumption of alcohol will be liable for disciplinary action, may be found guilty of gross misconduct, and may face summary dismissal.

Procedure

- All information relating to an employee's health including, but not limited to, matters involving alcohol, will be collected, held, and processed in accordance with the Company's [Employee] Data Protection Policy.
- In the event that an employee is diagnosed with an alcohol related problem the Company will treat it as a health matter. However, this does not excuse the employee from any of the disciplinary matters that may fall within the scope of the Company disciplinary policy.
- All alcohol related issues will be dealt with in a constructive and sympathetic manner. The individual responsible for all such issues is [***insert name and job title***] who will also provide any interested employees in confidence with details of where to seek more information or help.
- All requests for help or advice will be treated in the strictest confidence and all information gathered as a result will be held in accordance with the Company's [Employee] Data Protection Policy.
- After receiving any appropriate medical reports, the Company will provide support to any affected employees [and where necessary provide suitable treatment, to be paid for by the Company.] Where an employee agrees to follow a suitable course of action or treatment any disciplinary action may be suspended.
- The Company reserves the right to give affected employees lighter duties at the same rate of pay, or require them to take paid leave if it is deemed appropriate
- Following effective treatment and in the absence of any disciplinary action the Company will endeavour to return an affected employee to the same role previously fulfilled by the employee [***and where this is not possible to a suitable alternative***].

- In the event that an employee following successful treatment for an alcohol related problem suffers a relapse the Company [***will not make***] [***is under no obligation to make***] provision for any further treatment and the employee in question [***will***] [***may***] face summary dismissal.

- If it is considered that the working environment or culture is the cause or a contributor to an alcohol related problem, the Company will take all reasonably practical steps to ensure a reduction of such problems.

This policy has been approved and authorised by:

Name:

Position:

Date:

Signature:

[INSERT LOGO HERE]

Company Name

Communications, Email, Internet and Social Media Policy

Last updated date:

1. Introduction

1.1 This Communications, Email, Internet, and Social Media Policy applies to all staff members, contractors, and agents of [***insert name of Company***] a company registered in [***insert country of registration***] under number [***insert Company number***], whose registered office is at [***insert registered office address***] (the ***Company***) who use the communications equipment, computers, devices, and systems provided by the Company (***Users***).

1.2 Users are encouraged to use email and the internet at work as a fast and reliable method of communication with significant advantages for business.

1.3 In light of the fact that communications made by Users and their other activities online reflect upon the Company and are capable of creating a number of commercial, professional, and legal problems, this Policy is intended to clarify what the Company expects from Users and their responsibilities when using the Company's communications, email, and internet facilities (collectively, the ***Company's Internet and Communication Facilities***).

1.4 The Company's Internet and Communication Facilities include:

1.4.1 Telephone;

1.4.2 Fax;

1.4.3 Email;

1.4.4 Internet;

1.4.5 Intranet;

1.4.6 [***insert any additional items***]

1.5 [Whilst the Company's Internet and Communications Facilities are made available to Users for the purposes of the business, a certain amount of limited personal use is permitted insofar as such personal use is consistent with this Policy and the duties of the User.**]**

1.6 In addition to this Policy, when using the Company's Internet and Communications Facilities, Users must also comply with other Company Policies including the Company's Data Protection Policy, Equal Opportunities and Diversity Policy, and Harassment and Bullying Policy **[*add other policies if required*]**.

2. General Principles

There are certain general principles that should be borne in mind when using any type of communication, be it external or internal, including hard copy letters, memos, and notices. The Company expects all Users to:

2.1 Use the Company's Internet and Communication Facilities, and non-electronic facilities including but not limited to Company letterheads and stationery, responsibly and professionally and at all times in accordance with their duties;

2.2 Be mindful of what constitutes confidential or restricted information and ensure that such information is never disseminated in the course of communications without express authority;

2.3 Be mindful of what constitutes personal data and ensure that personal data relating to [***any*** individuals***, eg customers, colleagues***] is never disseminated in the course of communications unless it is used in accordance with the Company's Data Protection Policy and with express authority;

2.4 Ensure that they do not breach any copyright or other intellectual property right when making communications;

2.5 Ensure that they do not bind themselves or the Company to any agreement without express authority to do so; and

2.6 Be mindful of the fact that any communication may be required to be relied upon in court, to the advantage or the detriment of the individual or the Company, and to conduct their use of communication systems and equipment accordingly.

2.7 The viewing, transmission, downloading, uploading, or accessing in any way of any of the following material using the Company's Internet and Communications Facilities will amount to gross misconduct with the possibility of summary dismissal:

2.7.1 Material which is pornographic, sexist, racist, homophobic, or any other discriminatory or otherwise offensive material;

2.7.2 Illegal or criminal material, including material which breaches copyright or any other intellectual property right;

2.7.3 Any material which has the object or effect of causing harassment to the recipient;

2.7.4 Material which the User knows, or reasonably ought to know, is confidential or restricted information and which they are not authorised to deal with;

2.7.5 **[**Subject to paragraph 3.7, any**] OR [**Any**]** website or online service which the Company has blocked access to.

3. Internet Use

3.1 The Company provides access to the internet for the sole purpose of business and to assist Users in the performance of their duties. **[**Use of the internet for personal purposes is strictly prohibited.**] OR [**However, the Company recognises that Users may need to use the internet for personal purposes and such use is permitted provided it is reasonable and **[**does not interfere with the User's performance of their duties**] OR [**is outside of normal working hours or during a break.**]]** Users may be asked to justify the amount of time they have spent on the internet or the sites they have visited.

3.2 Users must not use the internet to gain or attempt to gain unauthorised access to computer material or private databases, including restricted areas of the Company's network. Nor must they intentionally or recklessly introduce any form of malware, spyware, virus, or other malicious software or code to the communications equipment or systems of the Company.

3.3 Users must not access or attempt to access any information which they know or reasonably ought to know is confidential or restricted.

3.4 Users must not access or use personal data online in any manner that is inconsistent with the Company's Data Protection Policy.

3.5 Users must not download or install any software without the express permission of [***insert name and job title***].

3.6 In accordance with paragraph 2.7, Users must not attempt to download, view, or otherwise retrieve illegal, pornographic, sexist, racist, offensive, or any other material which is in any way in bad taste or immoral. Users should note that even material that is legal under UK law

may nonetheless be in sufficiently bad taste to fall within this definition. As a general rule, if any person might be offended by any content, or if that material may be a source of embarrassment to the Company or otherwise tarnish the Company's image, viewing that material will constitute a breach of this Policy. Any such attempt will constitute a disciplinary offence and in addition to internet access being reviewed, reduced, or withdrawn, may be subject to disciplinary action or summary dismissal.

3.7 [Certain websites are blocked and cannot be accessed using the Company's Internet and Communication Facilities **[**during normal business hours**]**. If a User has a genuine and specific business need to access a blocked site, they must contact [***insert name and job title***].

4. Social Media Use - General Principles

4.1 This section of this Policy addresses the use by Users of all types of social network and social media platforms including, but not limited to, Facebook, Twitter, LinkedIn, Google+, Pinterest, Tumblr, Instagram, YouTube **[*insert other examples*]** (collectively, ***Social Media***).

4.2 The purpose of this part of Policy is to minimise the various risks to the Company presented by Social Media usage.

4.2.1 There are certain general principles that all Users should keep in mind when using Social Media [***, whether for personal use or***] for authorised work-related purposes. All Users must:

4.2.2 Use Social Media responsibly and professionally, and at all times in accordance with their duties;

4.2.3 Be mindful of what constitutes confidential, restricted, or other proprietary information and ensure that such information is never disseminated over Social Media without the express consent of **[**the Company**]** **OR** [***insert name and job title***];

4.2.4 Be mindful of what constitutes personal data and ensure that personal data relating to [***insert individuals, eg customers, colleagues***] is never disseminated over Social Media unless it is used in accordance with the Company's Data Protection Policy and with express authority;

4.2.5 Ensure that their use of Social Media does not breach any other of the Company's policies including, but not limited to, its Data Protection Policy, Equal Opportunities and Diversity Policy, and Harassment and Bullying Policy **[*add a reference to any other relevant policies if necessary*]**;

4.2.6 Ensure that their use of Social Media does not breach any other laws, regulatory requirements, or other applicable rules set out by regulatory bodies and other organisations **[**including, but not limited to, [insert any relevant regulatory bodies or trade association**]**;

4.2.7 Ensure that they do not breach any copyright or other intellectual property rights when using Social Media;

4.2.8 Be mindful of the fact that any communication may be relied upon in court, to the advantage or detriment of the individual or the Company and conduct their use of Social Media accordingly.

4.3 If a User is unsure as to the appropriateness of a posting or other content they wish to publish, they should speak to [***insert name and job title***] at the earliest opportunity to seek clarification.

4.4 If a User sees any content on Social Media that disparages or otherwise reflects poorly on

the Company, such content should be reported to [***insert name and job title***].

5. **Personal Social Media Use**

[Users may use Social Media for personal purposes occasionally during work hours **[**for example, during breaks**]** provided that such usage complies with the provisions of this Policy and provided that it does not interfere with their work responsibilities or productivity.**]**

OR

[Users may not use Social Media for personal purposes at any time during work hours on or via the Company's Internet and Communication Facilities **[**or on computers, mobile devices, or other communications equipment belonging to themselves, whether via the Company network or otherwise**].]**

6. **Business Social Media Use**

6.1 Certain Users may from time to time be required to use Social Media on behalf of the Company. Users should only do so with the authorisation of their [***insert name and job title***], in accordance with instructions issued by [***insert name and job title***], and in accordance with this Policy.

6.2 Use of Social Media for business purposes must comply with the provisions of this Policy at all times.

6.3 Users using Social Media on behalf of the Company may from time to time be required to interact with other internet users via Social Media, for example, in response to posts or enquiries regarding the Company. Unless the instructions issued to that User (see paragraph 6.1) specifically authorise the User to respond without further approval, the User may not respond to any such communications without the prior approval of [***insert name and job title***]. In any event, no User using Social Media on behalf of the Company should respond to such communications, with or without prior approval, without first consulting the relevant individual and/or department unless they are fully knowledgeable of the relevant topic and suitably qualified to respond.

6.4 **[**Social Media contacts made during the course of business are to be treated as confidential information belonging to the Company.**]**

6.5 **[**Before using Social Media on behalf of the Company, Users may require training in order to do so, or may be required to demonstrate that they have already received suitable training, either from the Company or from a previous employer or other organisation.**]**

7. **Acceptable Use of Social Media**

7.1 If a User makes any posting, contribution, or creation or publishes any other content which identifies or could identify the User as an employee, contractor, agent, or other member or associate of the Company, or in which the User discusses their work or experiences relating to the Company, the User must at all times ensure that their conduct is appropriate and consistent with their contract of employment and the corporate image of the Company, and should bear in mind that the User owes a duty of fidelity to the Company.

7.2 Unless specifically instructed to do so [***insert name and job title***], Users should make it clear that they are posting on Social Media as themselves, not as the Company, and that all opinions and ideas expressed on Social Media by that User are those of the User and do not necessarily reflect the views of the Company.

7.3 Unless using Social Media on behalf of the Company, Users should not use any Social Media accounts belonging to (or otherwise associated with) the Company.

7.4 Company email addresses may **[**not be used to sign up to any Social Media websites**] OR [**only be used to sign up to Social Media websites for work-related purposes**] OR [**be used to sign up to Social Media websites for work-related or personal purposes, however Users should be aware that their Company email address will cease to function should they cease to work for or with the Company and may result in the Social Media account(s) in question being inaccessible**]**.

7.5 Users should always be respectful to others when using Social Media and should always be mindful of the fact that their association with the Company may be known to anyone at any time. The conduct of all Users on Social Media may reflect on the Company, whether positive or negative. This applies whether a User is using Social Media for business purposes or for personal purposes, whether during workings hours or otherwise.

7.6 If a User is unsure as to the appropriateness of a posting or other content they wish to publish, they should speak to [***insert name and job title***] at the earliest opportunity to seek clarification.

8. Unacceptable and Prohibited Use of Social Media

8.1 Users must refrain from doing anything on Social Media or any other websites that defames, disparages, or otherwise brings into disrepute, the Company, a User's superiors, a User's colleagues, or other related third parties. This includes, but is not limited to, making false or misleading statements and impersonating colleagues or third parties.

8.2 Users must ensure that their use of Social Media does not damage the Company, its interests, or its reputation, whether directly or indirectly, in any way.

8.3 As under paragraph 7.2, unless specifically instructed to do so, Users must not represent themselves on Social Media as the Company or as posting on behalf of the Company.

8.4 Users may not share the following on Social Media unless specifically authorised to do so by [***insert name and job title***]:

8.4.1 Confidential information;

8.4.2 Commercially sensitive or other proprietary business information belonging to or about the Company or any of its employees, contractors, agents, or other affiliated third parties and organisations;

8.4.3 Personal data relating to [***insert individuals, eg customers, colleagues***].

8.5 Users may not use any intellectual property belonging to the Company on Social Media (including, but not limited to, trademarks and logos) unless specifically authorised to do so by [***insert name and job title***].

8.6 Users may not add contacts made during the course of their duties to their personal Social Media accounts **[[**without the authorisation of [***insert name and job title***] and**]** without the express consent of the individuals involved**]**.

9. Company Email Use

9.1 The email address with which Users are provided by the Company (ending in the suffix [***@emailaddress***]) is provided for business purposes in order to facilitate information sharing and timely communication with [***insert recipients - customers, clients, colleagues***]. Any Company business which is conducted via email must be conducted using Company email and is under no circumstances to be conducted through any other personal email address or account.

9.2 Users should adopt the following points as part of best practice:

9.2.1 Before communicating via email, Users should satisfy themselves that it is the most suitable mode of communication, particularly where time is of the essence;

9.2.2 Ensure that the email contains the Company disclaimer notice. This should be added automatically by the email client. If it is not, Users should speak to [***insert name and job title***] immediately;

9.2.3 All emails should contain the appropriate business reference(s), either in the subject line or in the body of the text;

9.2.4 Emails should be worded appropriately and in the same professional manner as if they were a letter;

9.2.5 Users should be careful not to copy an email automatically to everyone copied in to the original message to which they are responding as this may result in inappropriate or unlawful disclosure of confidential information and/or personal data;

9.2.6 Users should take care with the content of emails, in particular avoiding incorrect or improper statements and the unauthorised inclusion of confidential information or personal data. Failure to follow this point may lead to claims for discrimination, harassment, defamation, breach of contract, breach of confidentiality, or personal data breaches;

9.2.7 All emails should be proofread before transmission, which includes ensuring that any attachments referred to in the text are actually attached and are correct and the intended recipients' email addresses are correct;

9.2.8 If an important document is transmitted via email, the sender should telephone the recipient to confirm that the document has been received in full;

9.2.9 **[**All emails received relating to a [***insert subject titles***] should be printed and filed in the appropriate place;**]**

9.2.10 **[**No email relating to a [***insert subject titles***] should be deleted unless a hard copy has first been printed and filed.**]**

9.3 Users must not email any business document to their own or a colleague's personal web-based email accounts. **[**Furthermore, Users must not email any business document to any [***insert recipients - customers, clients, colleagues***] web-based email address unless specifically permitted to do so by the recipient.**]**

9.4 **[**Use of Company email for any personal matter is prohibited as it places additional strain on the Company's communications facilities.**]** ***OR*** **[**Users may use Company email for personal purposes, provided that such use is kept to a minimum and does not interfere with the performance of the User's duties. In any case Users are not permitted to use their Company email address to subscribe to any newsletters or to receive any marketing, as this will result in extra unnecessary burden being placed upon the Company's communications systems. All personal emails should be labelled "personal" in the subject line.**]**

9.5 **[**If Users do use Company email for personal reasons, they will be deemed to agree to the possibility that any emails sent or received may be subject to monitoring in accordance with Part 14 of this Policy.**]**

9.6 Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, pornographic, or otherwise inappropriate material in emails. If any User feels that they have been or are being harassed or bullied, or if they are offended by material received in an email from another User, they should inform [***insert name and job title***].

9.7 Users should at all times remember that email messages may have to be disclosed as evidence for any court proceedings or investigations by regulatory bodies and may therefore be prejudicial to both their and the Company's interests. Users should remember that data which appears to have been deleted is often recoverable. If secure deletion is required, for example, where an email contains confidential information or personal data, Users should follow the steps set out in the Company's ***[insert titles of relevant policies***].

10. **Personal Email Use**

[Users are permitted to access and use their personal email accounts only to the extent that such use is reasonable and [does not interfere with the User's performance of their duties**] OR [**is outside of normal working hours or during a break**].]**

OR

[Users are not permitted to access their personal email accounts via the Company's Internet and Communications Facilities.**]**

11. **Company Telephone System Use**

11.1 The Company's telephone lines and mobile phones issued by the Company are for the exclusive use by Users working on the Company's business. Essential personal telephone calls regarding Users' domestic arrangements are acceptable, but excessive use of the Company's telephone system and/or mobile phones for personal calls is prohibited. Acceptable use may be defined as no more than [***insert amount of time***] of personal calls in a working day. Any personal telephone calls should be timed to cause minimal disruption to Users' work.

11.2 Users should be aware that telephone calls made and received on the Company's telephone lines **[**and mobile phones issued by the Company**]** may be routinely monitored to ensure customer satisfaction or to check the telephone system is not being abused.

11.3 If the Company discovers that the telephone system or a mobile phone issued by the Company has been used excessively for personal calls, this will be treated as a disciplinary matter and will be handled in accordance with the Company's disciplinary procedures.

12. **Personal Mobile Phone Use**

12.1 Essential personal telephone calls regarding Users' domestic arrangements are acceptable, but excessive use of Users' own mobile phones for personal communications (including, but not limited to, calls, messaging, emailing, and web browsing) is prohibited. In order to avoid disruption to others, mobile phones should be set to silent during normal working hours.

12.2 Any personal telephone calls on Users' own mobile phones should be timed to cause minimal disruption to Users' work and to colleagues working nearby.

13. **Security**

13.1 The integrity of the Company's business relies on the security of the Company's Internet and Communications Facilities. Users bear the responsibility of preserving the security of Company's Internet and Communications Facilities through careful and cautious use. In addition to the general provisions contained in this Policy, Users must also comply with the Company's ***[insert titles of relevant policies***].

13.2 **[**Access to certain websites and online services via the Company's Internet and Communications Facilities is blocked. Often the decision to block a website or service is based on potential security risks that the site or service poses. Users must not attempt to circumvent any blocks placed on any website or service by the Company.**]**

13.3 Users must not download or install any software or program without the express permission

of [***insert name and job title***] and are reminded of paragraphs 3.2 and 3.5 of this Policy.

13.4 Users must not delete, destroy, or otherwise modify any part of the Company's Internet and Communications Facilities (including, but not limited to, hardware and software) without the express permission of [***insert name and job title***].

13.5 Users must not share any password that they use for accessing the Company's Internet and Communications Facilities with any person, other than when it is necessary for maintenance or repairs by [***insert name and job title or department***]. Where it has been necessary to share a password, the User should change the password immediately when it is no longer required by [***insert name and job title or department***]. Users are reminded that it is good practice to change passwords regularly. **[**Further guidance on passwords is contained in the Company's ***[insert titles of relevant policies***].**]**

13.6 Users must ensure that confidential information, personal data, and other sensitive information is kept secure. The security of personal data in particular is governed by the Company's Data Protection Policy, which Users must comply with at all times when handling personal data. Workstations and screens should be locked when the User is away from the machine and hard copy files and documents should be secured when not in use.

13.7 If a User has been issued with a laptop, tablet, smartphone, or other mobile device, that device should be kept secure at all times, particularly when travelling. Mobile devices must be password-protected **[**and, where more secure methods are available, such as fingerprint recognition, such methods must be used**]**. Confidential information, personal data, and other sensitive information stored and/or accessed on a mobile device should be kept to the minimum necessary for the User to perform their duties. Users should also be aware that when using mobile devices outside of the workplace, information displayed on them may be read by unauthorised third parties, for example, in public places and on public transport.

13.8 **[**Users using Company-issued mobile devices (as outlined above in paragraph 13.7) must not connect such devices to public wi-fi networks, for example, in cafes, restaurants, and on public transport **[**without the express approval of a particular network from [***insert name and job title***].**]]**

13.9 When opening email from external sources Users must exercise caution in light of the risk malware, spyware, viruses, and other malicious software or code pose to system security. Users should always ensure that they know what an attachment is before opening it. If a User suspects that their computer has been affected by a virus they must contact [***insert name and job title***] immediately.

13.10 **[**No equipment or device that has not been issued by the Company may be connected to or used in conjunction with the Company's Internet and Communications Facilities without the prior express permission of [***insert name and job title***]. Such permission may be conditional on the testing and/or inspection of the equipment or device in question.**]**

14. Monitoring

14.1 To the extent permitted or required by law, the Company may monitor Users' use of the Company's Internet and Communications Facilities for its legitimate business purposes which include (but are not necessarily limited to) the following reasons:

14.1.1 To ensure Company policies and guidelines are followed, and standards of service are maintained;

14.1.2 To comply with any legal obligation;

14.1.3 To investigate and prevent the unauthorised use of the Company's Internet and Communications Facilities and maintain security;

14.1.4 If the Company suspects that a User has been viewing or sending offensive or illegal material (or material that is otherwise in violation of this Policy);

14.1.5 If the Company suspects that a User has been spending an excessive amount of time using the Company's Internet and Communications Facilities for personal purposes.

14.2 Users should be aware that all internet and email traffic data sent and received using the Company's Internet and Communications Facilities is logged, including websites visited, times of visits, and duration of visits. Any personal use of the internet will necessarily therefore be logged also. Users who wish to avoid the possibility of the Company becoming aware of any political or religious beliefs or affiliations should avoid visiting websites at work which might reveal such affiliations. By using the Company's Internet and Communications Facilities for personal use, Users are taken to consent to personal communications being logged and monitored by the Company. The Company shall ensure that any monitoring of Users' use of the Company's Internet and Communications Facilities complies with all relevant legislation including, but not limited to, the GDPR (EU Regulation 2016/679 General Data Protection Regulation) and the Human Rights Act 1998. **[**For further information, please refer to the Company's ***[insert titles of relevant policies***].**]**

14.3 When monitoring emails, the Company will normally restrict itself to looking at the address and heading of the emails. However, if it is considered necessary, the Company may open and read emails. Users should be aware that sensitive and confidential communications should not be sent by email because it cannot be guaranteed to be private. Users are reminded that any permitted personal emails should be marked as "personal" in the subject line.

15. **Recruitment**

[The Company may use internet searches to carry out due diligence as part of its recruitment process. In these circumstances, the Company will act in accordance with its equal opportunities and data protection obligations.**]**

OR

[The Company does not permit the use of internet searches for recruitment purposes.**]**

16. **Misuse and Compliance**

16.1 Any User found to be misusing the Company's Internet and Communications Facilities will be treated in line with the Company's Disciplinary Policy and Procedure. Misuse of the internet can, in some cases, amount to a criminal offence.

16.2 Where any evidence of misuse of the Company's Internet and Communications Facilities is found, the Company may undertake an investigation into the misuse in accordance with the Company's Disciplinary Policy and Procedure. If criminal activity is suspected or found, the Company may hand over relevant information to the police in connection with a criminal investigation.

[INSERT LOGO HERE]

This Policy has been approved and authorised by:

Name:

Position:

Date:

Signature:

Company Name

Policy on Bringing Employee's Own Devices to Work (*BYOD*)

Last updated date:

1. Introduction

This policy applies to employees who work remotely or who bring their computers and/or other electronic devices, such as smartphones, mobile phones and tablets into work. This Policy on Bringing Employees' Own Devices to Work (***BYOD***) is intended to protect the security and integrity of any personal data and the Company's technology infrastructure. It should be read in conjunction with the Company's Communications, Email and Internet Policy.

[With the prior agreement of the [***insert name and job title***], all**]**/All employees are permitted to use their own devices for work-related purposes. However, employees must agree to the terms and conditions set down in this policy in order to be able to connect their devices to the company network.

2. Acceptable Use

The employee is expected to use his or her devices in an ethical manner at all times in accordance with the Company's Communications, Email and Internet Policy and Data Protection Policy.

The company defines acceptable use of employee's own devices as:

- activities that directly or indirectly support the business of the Company
- [reasonable and limited personal communication or recreation, such as reading or game playing.]

Devices' camera and**/**or video capabilities must be disabled while on-site.

Devices may not be used at any time to:

- Store or transmit illicit materials
- Store or transmit proprietary information belonging to another company
- Harass others
- [Engage in outside business activities]

Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, [***include any other***] and documents.

Employees should be aware that any personal device used at work may be subject to discovery in litigation and may be used as evidence in any action against the Company (see also 5.3 below).

The General Data Protection Regulation (*GDPR*)

[***Insert Company Name***] is the data controller in respect of work-related personal data that is held on personal devices. [***Insert name and job title***] is the Company's data protection officer and is responsible for the implementation of this policy.]

The GDPR requires the Company to process personal data in accordance with the six data protection principles. Employers must:

- Process personal data fairly, lawfully and transparently
- Obtain and process data only for one or more specified and lawful purposes
- Ensure that data is adequate, relevant and limited to what is necessary
- Ensure that data is accurate and kept up-to-date
- Not keep data longer than necessary
- Take appropriate technical and organisational measures against accidental loss or destruction of, or damage to, personal data.

3. Special Category Data

"Special category data" is information about an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or philosophical beliefs
- trade union membership
- physical or mental health or condition
- sex life or sexual orientation.

EITHER

[Employees must not process special category data on a personal device. If an employee has any special category data on his or her device, he or she must have it permanently deleted from the device.]

OR

[Employees may store special category data on a personal device provided that the device has a sufficiently high level of encryption.]

4. Employees' Obligations in respect of BYOD

4.1 ***Security***

- In order to prevent unauthorized access, devices must be password protected using a strong password
- Any device used must lock itself with a password or PIN if it is idle for five minutes
- Any device used must be capable of locking automatically if an incorrect password is entered after several attempts
- Employees must ensure that, if they transfer data, they do so via an encrypted channel e.g. a VPN

- Employees must not download unverified apps that may present a threat to the security of the information held on their devices

- Employees should not use unsecured networks

- The loss of a device used for work-related activities must be reported at the earliest opportunity to [***insert name and job title***]

- Employees must report data breaches to ***insert name and job title***] immediately.

4.2 ***Devices and Support***

- Devices must be presented to ***insert name and job title***] for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before employees can access the network.

4.3 **Cooperation with subject access requests**

Any individual whose personal date is held by the Company has the right to make a subject access request. Consequently, the Company may have to access your device in order to retrieve any data that is held on it about the individual. You must allow the Company to access the device and carry out a search for information about an individual that may be held on the device.

4.4 **Retention of Personal Data**

Employees must not keep personal data for longer than necessary for the purpose for which it is being used unless there is a requirement to retain it for longer in order to comply with a legal obligation.

4.5 **Deletion of Personal Data**

- Employees must ensure that, if they delete information from a device, the information must be permanently deleted rather than left in the device's waste management system.

- If removable media, e.g. a USB drive or CD, is used to transfer personal data, employees must ensure that the personal data is deleted after the transfer is complete.

4.6 **End of Employment**

Prior to the last day of employment with the Company, all employees must delete work-related personal data on his/her own device.

4.7 **Third-Party Use of Devices**

Employees must ensure that, in the event of friends or family using their devices, they are not able to access any work-related personal information by, for instance, password-protecting the information.

5. Monitoring

As part of its obligations under the GDPR, the Company will monitor data protection compliance in general and compliance with this policy in particular. The monitoring is in the Company's legitimate interests to ensure compliance with this policy and to ensure that the Company is complying with its

obligations under the GDPR.

Before any monitoring is undertaken, the Company will identify the specific purpose of the monitoring.

Monitoring will consist of: [***insert methods of monitoring***].

6. Non-Compliance

Any employee found to be breaching this policy will be treated in line with the Company's usual disciplinary procedure. Breaches of this policy could result in disciplinary action up to, and including, dismissal. Employees should be aware that they may incur personal criminal liability for breaches of this policy.

7. Review and Training

The Company will provide data protection training to all employees on a regular basis.

This BYOD policy will be reviewed on an annual basis.

This policy has been approved and authorised by:

Name:

Position:

Date:

Signature:

Company Name

Notice Periods Policy

Last updated date:

1. Introduction

The purpose of the Notice Periods Policy is to outline the Company's requirements for notice of termination of employment, either by the employee or the Company. It does not form part of the employees' terms and conditions of employment and may be varied, withdrawn or replaced by the Company.

2. Principles

2.1 Resignation

An employee who resigns must provide the Company with his or her written notice of resignation. An employee who resigns will be required to work his or her full contractual notice unless otherwise agreed.

The last day of service for pay purposes will be quoted in all letters accepting resignation and will be the last working day on which the employee attends work or is on paid leave. If an employee does not work his or her full contractual notice period without the Company's prior authorisation, the employee will not be paid for the part of the notice period that has not been worked.

[*The Company may deduct from an employee's final salary payment costs incurred on account of the employee failing to work his or her full notice period.*]

2.2 Dismissal

An employee whose appointment is terminated for any reason will be provided with a written statement of the reasons for the dismissal. The last day of service for pay purposes will be quoted in all letters terminating service and will be the last working day on which the employee attends work or is on paid leave. Where the Company dismisses an employee, it will give the employee his or her full contractual notice and will require the employee to work his or her notice period unless otherwise agreed.

If the Company dismisses an employee without notice, for example in cases of gross misconduct, the Company will explain the reasons for its decisions.

2.3 Redundancy

Where the Company dismisses an employee by reason of redundancy, it will give the employee his or her full contractual notice and will require the employee to work his or her notice period unless otherwise agreed.

2.4 Retirement

An employee who retired must provide the Company with his or her written notice of retirement in accordance with the notice period set down in his or her contract of employment. The employee is required to work their notice unless otherwise agreed.

3. Notice Periods

Subject to employees' terms and conditions of employment, which may set out a longer notice period, **[*following the probationary period*]** the Company will give employees one week's notice to terminate their contract of employment, with an additional week's notice per completed year of service after two years' continuous service, up to a maximum of 12 weeks.

After the employee's request and with the agreement of the employee's line manager, the employee's notice period may be waived or reduced. In these circumstances, the Company will not pay the employee for the part of the notice period that he or she is not working. The employee will be asked to sign a letter confirming the agreement that has been reached.

4. Rights and Obligations During the Notice Period

During the notice period, the contract of employment particulars will remain in force and the employee will continue to receive full pay and benefits.

The employee remains bound by all obligations and restrictions expressly set out or implied in his or her contract of employment and must not take up employment elsewhere. The Company expects the employee to conduct him or herself in an entirely appropriate manner during the full period of notice. This applies no matter who gave notice to terminate the contract of employment and for whatever reason.

5. Return of Company Property

On termination of employment for whatever reason, employees must deliver up to the Company all property, documentation, records, customer lists, client/prospect database information, memory sticks, magnetic discs, tapes or other software media belonging to the Company which may be in the employee's possession. Employees shall not, without the express written consent of the [***insert name and job title***], retain any copies. If so required by [***insert name and job title***], employees will sign a statement confirming that he or she has complied with the requirement.

If the employee fails to return any Company property by the required date, the Company will withhold the whole or any part of any pay due from the Company to the employee up to the current market value of the property not returned, i.e. based on the value of the property at the time that it is not returned and no on a replacement cost basis.

6. Garden Leave

If an employee is placed on garden leave for all or part of the notice period, he or she will not be allowed to come to work, i.e. he or she must stay away from the workplace during the garden leave period.

If an employee is placed on garden leave, he or she:

a) must not attend his or her place of work or any other premises of the Company or any associated company, unless otherwise requested by the company;

b) may be asked to relinquish immediately any offices he or she holds in the Company or any associated Company;

c) may or may not be required to carry out his or her normal duties during the remaining period of his or her employment. However, the employee must still be available to be contacted by the Company;

d) must return to the company all documents, software, equipment, property and other materials (including copies) belonging to the Company or associated company containing confidential information;

e) must not, without the prior written permission of the Company, contact or attempt to contact any client, customer, supplier, agent, professional adviser, broker, or banker of the Company or any associated company or any employee of the Company or any associated company; and

f) must not have any contact with another organisation, typically a competitor, during the garden leave period.

If the employee is placed on garden leave, his or her contract of employment will continue in force until the end of the notice period. This means that, during the garden leave period, he or she will:

a) continue to receive full pay and benefits (with the exception of benefits that are given to allow the employee to do his or her job, such as a work mobile phone or company car) in the normal way;

b) remain bound by all the obligations and restrictions set out in his or her contract of employment; and

c) not be permitted to take up other employment during the garden leave period.

7. **Pay in Lieu of Notice**

The Company may make a payment in lieu of notice for all or any part of an employee's notice period on termination of his or her employment (rather than have the employee work out his or her notice period).

The employee will be paid the payment that he or she would have received if he or she worked out his or her notice period.

8. **Holiday During Notice Periods**

During the notice period, the Company may require employees to take annual leave accrued for that holiday year but not taken by the date of termination of employment.

If, on termination of an employee's employment, the employee has accrued annual leave that he or she has not taken, he or she will be paid in lieu of annual leave as part of his or her final salary payment.

If, on termination of an employee's employment, he or she has taken paid annual leave in excess of accrued entitlement, he or she will be required to reimburse the Company (by means of deduction from salary if necessary) in respect of this holiday.

9. **Deductions from Final Salary**

Any sums due to the Company may be deducted from any money owing to the employee on or after the termination of his or her employment.

This includes, but is not limited to, the following: [***list items that may be deducted from final salary***]

.

If the employee's final salary payment is insufficient to cover the sums owed to the Company the employee will enter in to a contract with the Company for the repayment of all sums owed.

This policy has been approved and authorised by:

Name:

Position:

Date:

Signature: