Your Logo

Company name
Registered
Address

R

Acceptable Use Policy

ICTSP-05

Classification: Internal

Organization	Companies
[Organization Name] (the "Organization")	[List companies here]

Document Governance

Version	1.0
Release Date	Date you release the policy
Document Owner	Information Security Team
Review Period	Annual
Next Review date	Typically 1 year after the release date but you should determine frequency of review based on your type of business and required risk-management as well as any specific regulatory requirements e.g. imposed by your regulator.

Version History:

Version	Date	Author	Changes
1.0	[Date]	[Full name]	Initial version

Reviewers:

Name	Role	Organisation / Team	Date Reviewed	Signature

Approvers:

Name	Role	Organisation / Team	Date Approved	Signature
[Full name]	CEO	Senior Management Team	[Date]	
[Full name]	Information Security Manager	Information Security Team	[Date]	

1 Introduction

1.1 Objectives

Email, messaging, texting, social networking and internet use are essential tools for the Organization to conduct business. However, if our communication tools are used inappropriately, this could cause harm to our Information Systems, our people, brand, commercial performance and could expose us to litigation or financial penalties.

The Organization makes its Information Systems available to Users and allows you to connect your Mobile Devices for business use in line with your role and responsibilities. Whilst we recognize that Users may occasionally need to use company email, messaging, social networking, and internet facilities for non-business related purposes, this should be done in line with this policy. This policy is not meant to impose unnecessary restrictions. The objective of this policy is to inform all users of the behaviours that are expected of them whenever they use an Information System or use a Mobile Device to access or connect to our Information Systems, or in circumstances where use of any other equipment, services, network or applications which could have an impact on our brand and reputation, our people or our customers.

This policy gives you an overview of what is appropriate and inappropriate with regards to the use of the following:

- Personal Use
- Prohibited Use
- Working from home and remote working
- Removable Media
- Personally Identifiable Information
- Mobile Device Security
- Use of the Internet
- Password Security and Protection
- Email Use
- Monitoring
- Data Protection and Security

1.2 Scope

This policy applies to all situations where the Users communicate externally about the Organization, or do anything else which may affect our Information Systems. This includes situations such as:

- Using an email account or equipment supplied by the Organization to access personal facilities or resources (including messaging, social networking, texting, blogging, Skype etc).
- Using company email, messaging, social networking and internet facilities
- Using a personal, publicly accessible account (e.g. social networking or blogging) to communicate to the public about the Organization
- Using your own or a third party device (e.g. a personal laptop or internet café) to use social media or networking applications or sites to communicate or participate in conversations which could impact the Organization

This policy will apply to any actions detailed in it even if such actions are carried outside of normal working hours.

1.3 Audience

This policy applies to all Employees, Consultants and any Third parties that the Organization has authorised to use its Information Systems (such as contractors, subcontractors, secondees and trusted suppliers). We refer to all of these people as ***Users*** in this policy.

1.4 Definitions

See *ICTSP-02 Information Security Policy Framework* for definitions.

2 Roles and Responsibilities

2.1 Employees

Employees must:

- Read this policy at least once a year, understand and comply with this policy.
- Report any noncompliance to this policy to their site manager or Information Security Team.

2.2 Staff Managers

Managers must:

- Read, understand and comply with this policy.
- Ensure that Users who report to them read this policy annually and understand and comply with this policy at all times.
- Report any noncompliance with this policy to the Information Security Team.

2.3 Third Parties

Third parties who are authorised to use or support our Information Systems must:

- Understand and comply with this policy.
- Ensure their subcontractors (involved in the delivery of service or goods to the Organization) comply with requirements of this policy.
- Report any non-compliance with this policy to the Information Security Team.

2.4 Relationship Managers

Employees who are responsible for managing Organization's relationship with Third Parties/Managed Service providers must:

- Ensure the requirements of this policy are embedded within Contracts and Agreements with third parties/managed service providers.
- Ensure that third parties/managed service providers read and understand this policy.
- Report any non-compliance with this policy by third parties/managed service providers to Information Security Team.

3 Personal use

Personal use must not:

- Interfere with, restrict the performance of or take priority over your work responsibilities and duties

- Bring the Organization into disrepute or have a negative impact on the Organization or undermine its brand and reputation
- Be excessive
- Fall within the “Prohibited Use” categories set out below

Must be:

- Lawful and conform to the provisions of this policy

4 Prohibited Use

4.1 Prohibited use of Organization’s Information Systems

Users must not knowingly use Information Systems, unless authorised, to download, upload, send, accept, retain, any material or software that:

- Encrypts messages, client information, data, or work-related files without the permission of Information Security Team and without taking appropriate measures to ensure that the Organization can access the encrypted information. Please refer to the Encryption Policy for more information.
- Enables the introduction or use of packet-sniffing software or password detecting software or tools unless it is an approved software by the Information Security Team.
- Enables access to restricted areas (“hacking”), or attempt or carry out any “hacking” activities (unless authorised by the Information Security Team).
- Is unlawful (e.g. illegally downloading pirated content). End Users must assume that all materials on the internet are copyright and/or patented unless specific notices state otherwise.
- Is intended to disrupt or degrade Organization’s Information Systems.

The following activities are strictly prohibited, with no exceptions:

- Deliberately subvert Organization’s security controls (e.g. using proxies, translation services to avoid Internet filtering).
- Insert media devices which are not secure into Organization’s Information Systems.
- Enable the provision of unauthorised access to the Organization information and information systems (e.g. providing unauthorised access to shared resources e.g. SharePoint sites, wiki sites, shared folders/drives).
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the organization.
- Unauthorised copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the organization or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting the organizations business, even if you have authorised access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Use the Organization's Information Systems to conduct commercial or charitable activities outside the scope of your role and responsibilities, (e.g. to sell or advertise unrelated third party goods or services or to run a charity or business activity), unless expressly approved by the appropriate Director.
- Access the Information Systems that are not within the scope of your work and responsibilities, such as reading or changing customer or personnel information without authorisation.

5. Working from home and Remote Working

Users working remotely must ensure that the connection is secure. Connectivity to the Organization's Information Systems should not be through public Wi-Fi or any insecure mechanism (e.g. free cloud WiFi).

6. Removable Media

Users must comply with the Information Classification Policy when using removable media (for example when copying Confidential or Secret information onto media you must use encryption and have a business justification).

7. Personally Identifiable Information

For Users accessing Personally Identifiable Information (including payment card data) via remote access, the ability to copy, move, and store this data onto local hard drives and removable electronic media is prohibited unless explicitly authorised for a defined business need.

8. Mobile Device Security

This will apply to all Mobile Devices that have the Organization's information on them, or are connected to the Organization's Information Systems.

- If your Mobile Device is lost or stolen, you must alert IT Helpdesk and Information Security Team immediately.
- You must always physically secure all Mobile Devices when leaving them unattended in line with the Secure Desk Policy.
- All Mobile Devices and computers that you use to connect to Information Systems must be properly authenticated.
- We reserve the right to delete all information relating to the Organization from your Mobile Device if your Mobile Device is:
    - Used to breach any of our policies.
    - Found to contain or is transmitting malware onto our network or IT systems (such as a virus).
    - Lost or stolen.
    - If you leave the Organization and retain your Mobile Device.

9. Secure use of Internet

Users must use:

- organization's Information Systems to only browse sites that are known to be safe and which contain appropriate content for display at work.

Users must not:

- Knowingly download, install, or run any software on any of Organization's Information Systems which is not listed as approved software or which may contain malware.
- Connect Organization's Mobile Devices to insecure wireless networks (e.g. public Wi-Fi networks, or private Wi-Fi systems that are not password protected).
- Download or install files or software from unauthorised sites.
- Click on pop ups, adverts or banners in browsers, unless it is part of a business approved tool.
- Utilise services that may store, transmit, process or access Organization's classified information, that have not been approved by the Information Security Team.

10. Password Security & Protection

Users must:

- Change passwords when prompted to by the Information Security Team.
- Report any potential password compromise to Information Security Team.
- Transmit usernames and passwords through two separate methods whenever feasible (for example one via email and one via text message).

Users must not:

- Share or reveal their passwords to anyone else.
- Allow systems or applications to store passwords or cache credentials.
- Write passwords down and store them where others may access them e.g. documentation, online (SharePoint, wikis, shared folder/drives).

11. Use of Email

Emails are corporate documents and remain the property of the Organization at all times. The Organization has a legal obligation to protect the confidentiality of company and customer information and may be prosecuted where we fail to do so. If you leave the Organization you should be aware that we will continue to retain any communications used during your employment in line with data protection law.

Users must:

- Adopt a professional style when communicating externally. External emails must be written to professional business standards equivalent to the style and manner expected of letters and memos written on company headed paper. While internal emails can be more informal, you must comply with all other aspects of this policy.
- Use email signatures in accordance with any company or departmental guidelines.
- Exercise due care in making sure that intended recipients are authorised to receive information contained in or attached to an email.
- Retain emails until no longer required for business purposes or to meet any legal or regulatory obligations.
- Retain all email messages relating to actual or threatened legal proceedings that you or the Organization may be involved in, until instructed otherwise. You must seek advice from the Senior Management Team before deleting such emails.
- Handle information in line with the Information Classification Policy.
- Whenever employee state an affiliation to the company, they must clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

Users must not:

- Open an email attachment or file unless you have identified the sender and the reason they are sending the attachment.

- Redirect work email which is Internal, Confidential or Secret to your personal email account.
- Forward suspicious emails with attachments or originate 'junk' or 'spam' emails unless it is to inform Information Security Team.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Send bulk emails or send to distribution lists when this is inappropriate or when a communication is relevant only to a limited number of Users unless prior approval has been given by your line manager.
- Forwarding bulk messages to parties outside the Organization (unless this has been expressly authorised through your working roles and responsibilities).
- Intercept or disclose, or assist in intercepting or disclosing, the private communications of anyone else (unless a member of the Senior Management Team authorises that).
- Be involved in any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Use of unsolicited email originating from within the organization networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted or connected via the organization's network.

Users should not:

- Use Organization’s Information Systems to communicate personal details which you do not wish to be known to the Organization.

12. Social Media and Blogging

- Blogging by employees, whether using the organizations property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the organizations policy, is not detrimental to the organizations best interests, and does not interfere with an employee's regular work duties. Blogging from the organizations systems is also subject to monitoring.
- The Classification policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited.
- Employees may also not attribute personal statements, opinions or beliefs to the organization when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the organization. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, the organizations trademarks, logos and any other intellectual property may also not be used in connection with any blogging activity.

13 Monitoring

The Organization is committed to respecting reasonable expectations of privacy concerning the use of the Organization’s Internet facilities. However, the Organization cannot guarantee complete

privacy. You should be aware that the law allows organisations to monitor and record their employees' communications in a number of circumstances.

This section specifies the circumstances in which the Organization may monitor Users telephone calls, text messages, faxes, emails, instant messages, and text messages where these communications are sent or received via Organization's Information Systems or a Mobile Device that is used to access Organization's Information Systems. We may also monitor any of your social networking activity that relates to the Organization.

13.1 Monitoring of emails and Internet use

The Organization may monitor the emails and Internet use of User as follows:

- Systematic routine monitoring of emails by scanning for content that is prohibited by this policy.
- Random monitoring for prohibited and excessive personal use.
- Systematic routine monitoring of internet use for illegal or other purposes prohibited by this policy.
- Specific targeted monitoring and of communications for legitimate business purposes including:
    - establishing facts relevant to the Organization's business (e.g. dealings with customers, suppliers and competitors);
    - training, quality control and monitoring of required business standards;
    - ensuring compliance with any regulatory or self-regulatory requirements ;
    - protecting Organization''s Information Systems and to ensure effective system operation (e.g. to intercept and prevent malware or to manage network traffic);
    - detecting the unauthorised use of Organization's Information Systems or of Mobile Devices connected to the Information Systems;
    - detecting and preventing crime;
    - accessing User emails, text messages, instant messages, letters or faxes where necessary to continue conducting business (e.g. checking email accounts to access business communications during the absence of a User;

13.2 Compliance with the law

The Organization will comply with all relevant legislation whenever we carry out any monitoring exercise, to ensure that the rights of Users are protected.

13.3 Monitoring process

Monitoring will be carried out either through an automated system and/or through approved personnel who have been trained and authorised to conduct such monitoring.

The Organization will retain information obtained through monitoring until it is no longer required to support the purposes outlined in this policy. The audit functions at the Organization may conduct periodic audits of User monitoring to ensure that appropriate standards are maintained.

13.4 Targeted monitoring of specified Users

The Organization will monitor specific individuals in exceptional circumstances only. The Senior Management Team must grant their express consent first, after consulting the Legal Counsel of the Organization.

Before conducting targeted monitoring, the Organizations must first conduct a risk assessment to consider any adverse impact upon the User balanced against any obligations to other email users, Organization's shareholders and customers, and the police or regulatory bodies.

14. Data Protection and Security

Information relating to the Organization's customers, employees and business operations is confidential and may be used and disclosed only where this is commensurate with your role and responsibilities, or where you are otherwise specifically authorised or instructed. You are legally responsible for making sure the confidentiality of proprietary, client, customer and employee information is protected at all times, and to protect it against unauthorised access, disclosure and use. Misuse of customer/employee personal information may result in disciplinary action.

Users can be criminally liable if they knowingly or recklessly disclose account and personal information about Organization's customers and personal information about employees. Therefore you must not disclose the email addresses or telephone numbers of other Users to 3rd parties unless the User has consented or where you reasonably believe the User would not object to such.

Users must not make any personal or inappropriate expressions of opinion or comments about our customers, third parties, partners, employees, products and services. All individuals have a right to see information held about them.

Users should only send information by email to persons or organisations as required to fulfil their role or where otherwise authorised or instructed by the Organization. Users should be aware that email is not a secure form of communication. If the contents of an email or any attachments are Confidential or Secret, then you must refer to the Information Classification Policy for guidance on appropriate markings and any encryption requirements.