Your Logo

Company name
Registered
Address

Acceptable Use Policy

Policy Extract only

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]	

Your Logo

Company name
Registered
Address

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

----------END OF EXTRACT----------