ACCEPTABLE USE POLICY - END USER AGREEMENT

*Revision: r1.0*

*Effective Date: dd-mm-yyyy*

*Classification: INTERNAL*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employee 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Employee Rights 4

2.2 Use of Electronic Devices 4

2.3 Electronic Communications 5

2.4 Regulatory Compliance 6

2.5 Clean Desk / Clear Screen 6

2.6 Tailgating 6

2.7 Copy Retention 6

3. Policy Compliance & Enforcement 7

3.1 Compliance Measures 7

3.2 Enforcement 7

4. Exception Process / Glossary 8

4.1 Exception Process 8

4.2 Glossary / Acronyms 8

5. Document Management 9

5.1 Document Revision Log 9

5.2 Document Ownership 9

5.3 Document Coordinator 9

5.4 Document Approvers 9

5.5 Document Distribution 9

6. End User Signature 10

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Objective

The objective of this policy is to outline the acceptable use of electronic and Intellectual Property assets at XXXX.

All employee and contractors must sign a copy of this document on hire, or the beginning of a signed contract (if applicable). Signature assumes that the employee or contractor has both read AND understood the contents, and will comply in full.

If any aspect is not understood, it is the individual’s responsibility to seek clarity, as ignorance of the Policy’s meaning will not be accepted in case of dispute or legal action.

## Scope

### Applicability to employee

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employee, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-002 - Acceptable Use Policy*
* *XXXX-POL-ALL-009 - Access Control Policy*
* *XXXX-PRC-ALL-007 - Incident Response Procedure*
* *Human Resources Employee Handbook*

# Policy Statements

## Employee Rights

* Employees are entitled to protection under the UK Data Protection Act of 2018.
* Employees may send and receive internal or external electronic mail or undertake web browsing as part of their role within the XXXX;
* Personal electronic mail should only be sent during personal time, e.g. lunch hour (Note: software may be used to monitor and/or limit activity);
* Employees must recognize that during the management of the network, employee files/logs may be viewed. In addition, if the employee is suspected of breaching the employees’ responsibilities outlined in this Policy or of criminal activity, that employees’ files/logs may be viewed to protect other employee, their rights, and maintain the integrity of the XXXX’s network;
* Should the security of the network be threatened, any employees’ files may be examined;
* While unwanted or unsolicited contact cannot be fully controlled, employee who receive threatening communications should bring them to the attention of their direct line manager;
* Employees must be aware that there are many services on the Internet that might be considered offensive to groups of employee, and therefore, employee must take responsibility for their own navigation of the network and the Internet, please refer to employees’ responsibilities below for further guidelines.

## Use of Electronic Devices

* Employees are responsible for the use of their account and they may not:

1. give anyone else access to that account;
2. use a computer account that was not assigned to them;
3. try in any way to obtain the password for another employees’ computer account.
4. attempt to disguise the identity of either the account or the system they are using in order to represent themselves as another employee.

* All employees are responsible for the security of their authentication credentials and should ensure no one else knows them. All employees will change their authentication mechanism in line with the *XXXX-POL-ALL-009 - Access Control Policy*;
* All employees should either lock or log off from any relevant electronic device if they intend to leave that device for any length of time. XXXX will assume in the first instance that any files saved in a employees’ personal area were saved by the named employee of that personal area;
* Employees must not use XXXX’s network in order to gain unauthorized access to remote computers;
* Employees may not view, download or transmit to or from any relevant company owned electronic device material that is illegal, pornographic, defamatory, obscene or malicious. XXXX will dismiss a/any employee found to have viewed, downloaded or transmitted such material;
* Internet browsing for personal reasons should only be undertaken during personal time;
* Employees must not deliberately perform an act that will disrupt the normal operation of the network. This includes, but is not limited to, tampering with components of the network, or interfering with the operational readiness of a computer;
* Employees must not run or install, or give to another, a program which is intended to or likely to result in the eventual damage of a file or computer system and/or the reproduction of itself. This includes, but is not limited to, the programs known as computer viruses;
* For XXXX provided devices, employees should follow the instructions contained in the *XXXX-PRC-ALL-006 - Incident Response Procedure*. If there is any doubt about the source of the program, file or e-mail to which a virus warning refers the program, file or e-mail must not be opened and the relevant personnel informed immediately;
* Employees should not open or download files unless absolutely sure they are from a reputable source;
* Application software may only be installed on company provided desktops and servers by, or with the permission of XXXX;
* Employees must abide by the terms of all software licensing agreements and copyright laws, and may not make copies of or make available on copyrighted material, unless permitted under license;
* Employees must not attempt to circumvent data protection schemes or exploit security loopholes;
* Employees must ensure that the transfer of data via external media (e.g. thumb-drive) is not likely to result in the eventual damage of a file, application or computer system;
* Disk space on servers is not limitless, therefore employees should maintain good housekeeping practices. This means deleting old, unwanted or duplicated files on a regular basis in order to keep disk spaced used to a reasonable level;
* Employees must not attempt to monitor another employees’ data communications, nor read, copy, change or delete another employees’ files or software without appropriate permission.

## Electronic Communications

* All employees must remember that electronic communications are like any other form of communication, i.e. insecure. employee should only send sensitive external or internal e-mail after careful consideration of its value to others. If employees wish to send sensitive e-mail this must be carried out with the consent of the recipient and other persons who may be named in the content of the e-mail;
* Employees may not disclose the contents of e-mails, attachments or any data held electronically by XXXX. Such files and data should be treated as confidential and privileged at all times.
* If employees receive an e-mail that has been wrongly delivered to their e-mail address, they should notify the sender of the message by redirecting the message to that person. If that e-mail contains sensitive information the employee must not disclose or use that information.
* Employees should check all e-mails, especially external communication, with the same care and attention given to letters sent on headed XXXX paper. Such communications should be written in accordance with the standards of any other form of written communication.
* Employees may not transmit to or from any computer or fax communications that are illegal, pornographic, defamatory, obscene or malicious. XXXX will dismiss a/an employee found to have viewed, downloaded or transmitted such material. If an employee receives an e-mail they consider illegal, pornographic, defamatory, obscene or malicious they should raise the issue with their direct line manager or HR.
* Whilst XXXX understands that it is not always possible to control the communications received it does expect its employees to ensure such senders of inappropriate material are requested to desist from sending such material in the future.
* Employees should not open e-mails or attachments from unknown sources without seeking advice from the appropriate resource.
* Employees must conduct all official engagements through the bank provided official channels, i.e XXXX emails, Microsoft teams, workflow applications, intranet sites etc
* XXXX will assume in the first instance that any e-mails being sent under a employees’ name were sent by that employee.
* If employees are sending attachments by e-mail they should ensure that the consent of the author of the attachment, if not a company employee, has been obtained, otherwise a/an employee could infringe the author’s copyright.
* XXXX retains the right to intercept, read and print out all internal and external, incoming and outgoing, e-mails from company owned or managed electronic devices.
* Signatures must be attached to all e-mails.

## Regulatory Compliance

Where applicable, employees with access to resources or data in-scope for regulatory compliance must comply with the specific intent of the regulation. Documentation, and relevant training, will be made available by XXXX leadership when applicable.

## Clean Desk / Clear Screen

All employees must follow a clean desk and clear screen policy and ensure that no paperwork or digital copy above INTERNAL is left unattended. All media must be stored in lockable cabinets or equivalent safe containers.

## Tailgating

All employees must swipe access badges to enter restricted areas and must never allow others to follow behind them unless they too have swiped their badge and received a positive response.

## Copy Retention

Employees should retain a copy of this document. It should be signed at the time of joining XXXX and a copy shall be retained in the personnel file of the employee.

# Policy Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Evidence of users review and acknowledgement of their understanding of XXXX Acceptable Use Policy and other related information security policies. | * New hire training user sign-off documentation * Electronic responses to periodic surveys or security awareness training |
| Evidence that users are complying with the concepts of acceptable use. | * Level of exceptions from management reviews and audits in violation of acceptable use |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Glossary / Acronyms

|  |  |
| --- | --- |
| XXXX | XXXX |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
| July 10, 2020 | Michael Oyerinde | r1.0 | Approval of new policy |
| dd-mm-yyyy | Michael Oyerinde | r1.0 | Approval by Executive Committee |

## Document Ownership

This Policy is owned by the Executive Committee.

## Document Coordinator

This Policy is coordinated by the CISO.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
| Executive Committee |  | dd-mm-yyyy |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff
* All approved third parties and vendors

# End User Signature

All users will confirm and accept they have read this policy and a record of their confirmation will be kept