# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 1.1 |  |  |  |
| 1.2 |  |  |  |

# Introduction

This policy applies to staff, contractors and volunteers at Organisation Name. It has been prepared by the Organisation ICT Dept Name/Other.

The organisation seeks to promote and facilitate the proper and extensive use of Information Communication Technology (ICT) resources, such as PCs, laptops, tablet devices and smart phones for the purpose of supporting the business activities of the organisation.

It is the responsibility of all users of ICT services across the organisation to read and understand this policy. This policy may be updated from time to time, to comply with legal and policy requirements.

This Acceptable Use Policy is intended to provide a framework governing the use of all ICT resources. Its aim is to protect all users of equipment belonging to the organisation and minimise such risks by providing clarity on the behaviours expected and required by us. It also outlines the consequences of breaching the policy.

# Scope

This policy applies to all users of ICT facilities across the Organisation Name. This includes staff, contractors, agency workers, partners, (for Parish/Town Councils) Councillors and others. All these users are bound by the provisions of the organisation’s policies in addition to this Acceptable Use Policy. This policy also addresses the use of the organisation’s ICT facilities accessed via resources not fully owned by the organisation, such as partner resources and the use of personal BYOD (‘bring your own device’) equipment.

The ICT facilities include hardware, software, data, storage, network access, telephony, printing, back- office systems and services and service provided by third parties including, online, Cloud and hosted services.

# Acceptable Use

Organisation Name’s network may be used for any legal activity that is in furtherance of the purpose, aims and policies of the organisation.

Users may use the organisation’s networks for personal use; however, this is not a right and must be exercised with discretion and moderation. Personal use must not interfere with the performance of duties and those of others. Users further accept that the organisation does not accept any liability, in part or whole, for claims arising out of personal use of the systems.

# Unacceptable Use

Organisation Name’s network is defined as all computing, telecommunication, and networking facilities provided by the organisation, with particular reference to all computing devices, either personal or organisation-owned, connected to systems and services supplied on-premises or remotely.

Unacceptable material includes data, images, audio and video files which are illegal under UK law or not in line with relevant policies, the values and relevant codes of conduct of the organisation.

The conduct of all users when using the ICT facilities (including the use of online and social networking platforms) should always be in line with relevant policies, the values and relevant codes of conduct of the organisation.

## **Unacceptable use of networks includes:**

1. Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material.
2. Creation or transmission of material which harasses, bullies or victimises any member of the organisation or a third party or which promotes discrimination on the basis of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex or sexual orientation.
3. Creation or transmission of material with the intent to defraud or which is likely to deceive a third party or which advocates or promotes any unlawful act.
4. Creation or transmission of unlawful or unacceptable material, or material that is defamatory, threatening, discriminatory, promotes extremist beliefs/attitudes or which has the potential to radicalise themselves or others.
5. Creation or transmission of Unsolicited or bulk email (spam), the forging of addresses or use of mailing lists other than for legitimate purposes related to the organisation’s activities. The forwarding of email to any other external/or personal account.
6. Creation or transmission of Material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party.
7. Creation or transmission of Material that brings the organisation into disrepute.
8. Using of another user’s details to access networked facilities and services.
9. Deliberate unauthorised access to networked facilities and services or attempts to circumvent the organisation’s security systems.
10. Pursuance of commercial activities for personal gain.
11. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
* Wasting staff effort or time unnecessarily on ICT management.
* Corrupting or destroying other users’ data.
* Violating the privacy of other users.
* Disrupting the work of other users.
* Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
1. Installation or use of unapproved or unlicensed software on managed devices.
2. Continuing to use an item of software, hardware or services after a notification that use should be ceased.
3. Other misuse of network resources, such as the intentional introduction of computer viruses, malware, or other harmful software.
4. Introduction of data-interception, password-detecting or similar software or devices to the organisation’s network.

# Monitoring

* 1. Organisation Name records and monitors the use of its ICT facilities, under the Regulation of Investigatory Powers Act (2000) for the purposes of:
* The effective and efficient planning and operation of the ICT facilities.
* Investigation, detection and prevention of infringement of the law, this policy or other policies.
* Investigation of alleged misconduct by staff.
	1. The organisation will comply with lawful requests for information from government and law enforcement agencies.
	2. Access to personal workspaces and email, will not normally be given to another member of staff unless authorised by a relevant head of service or manager, who will use their discretion.
	3. Where there is a requirement to access the account of another member of staff, authorisation must be obtained in writing from the relevant head or appropriate manager.
	4. If the request for access is related to an investigation, this should be managed wholly through the investigating officer who will work with ICT if approved by the data protection officer or the head of Human Resources or their nominee.
	5. Searches of ICT resources may be carried out in order to support investigations and information requests. This will be done in consultation with the organisation’s data protection officer. Information contained in these resources may be disclosed in line with the organisation’s obligations.

# Consequences of Policy Breach

In the event of any failure to comply with the conditions of this Acceptable Use Policy by a User, Organisation Name may in their sole discretion:

* Restrict or terminate a user’s right to use their ICT facilities.
* Withdraw or remove any material uploaded by that user in contravention of this Policy.
* Where appropriate, disclose information to law enforcement agencies and take any legal action against a user for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.
* Any disciplinary action, arising from breach of this policy, shall be taken in accordance with the the organisation’s disciplinary policy. Disciplinary action may ultimately lead to dismissal.

# Deviations from Policy

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the Head of ICT & Digital.