Acceptable Use Policy

Template

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

# Introduction

Information technology (IT) resources, such as PCs, laptops, tablet devices, and smartphones, constantly offer new and exciting ways of working and engaging the world. However, we must also be aware that improper use can impact the organisation, our colleagues, and our clients.

This Acceptable Use Policy (AUP) aims to protect all users of our equipment and minimise risks by providing clarity on the behaviours expected from employees. This policy also details:

* the consequences of breaching the AUP
* how to conduct our business and achieve compliance
* an evaluation of new business and technology requirements

# Purpose

The purpose of the AUP is to ensure that users understand their responsibility for the appropriate use of our IT resources. Understanding this will help users to protect:

* themselves
* our equipment
* our information
* our reputation

# Scope

The scope of this policy includes all our equipment, information and channels of communication. It covers:

* IT systems
* hardware
* software
* voice-telephony
* social media
* video
* email
* instant messaging
* internet and intranet use

Users’ personal information that’s processed by us is also subject to this policy.

# Applicability

The AUP applies to all users with access to information and IT systems. This includes

* employees
* volunteers
* contractors
* consultants
* business partners

# Acceptable use principles

All users will apply the following principles when accessing our information and IT systems.

## General principles

1. Confirm that you agree to this AUP and understand that breaching this policy may result in disciplinary procedures. This will before use of our equipment or information, and through use of our security code of conduct.
2. Be responsible for your own actions and act responsibly and professionally. This means following our standards of behaviour and respecting the organisation, your colleagues, volunteers, suppliers and clients.
3. Use information, systems and equipment in line with our security and information management policies.
4. Immediately report any breach of this AUP to your line manager and/or to the <role>. You’ll also comply with official procedures when a breach of the policy is suspected or reported.
5. Never undertake illegal activity, or any activity that would be harmful to our reputation or put staff and/or client data at risk.
6. Understand that both business and personal use will be monitored as appropriate.
7. Be aware that you can use the ‘Whistleblowing Policy’, and raise a concern if it’s believed that someone is misusing our information and technology.
8. Take part in education and awareness on security and using our information and technology. This includes being able to understand, recognise, and report threats, risks and incidents.

## User IDs and passwords

1. Protect user names, staff numbers, smart cards and passwords appropriately.
2. Create secure passwords following best practice guidance.
3. Do not logon to any system using another user’s credentials.
4. Remove your network access smart card and/or lock the screen when leaving temporarily devices that are in use.
5. Log out of all computer devices connected to the internal network during non-working hours.

## Managing and protecting information

1. Understand that you and our organisation have a legal responsibility to protect personal and sensitive information.
2. Ensure that all information is created, used, shared and disposed of in line with business needs. It should also be in compliance with the ‘Information Management Policy’ and ‘Information Asset Inventory’ guidance.
3. Do not attempt to access personal data unless there’s a valid business need that’s appropriate to your job role.
4. Comply with HR rules in respect of handling employee information.
5. Do not provide information in response to callers or emails whose identity you cannot verify.
6. Be careful not to be overheard, or overlooked, when conducting business in public areas.
7. Do not attempt to access, amend, damage, delete or distribute another person’s files, emails, communications, or data without the appropriate authority.
8. Do not attempt to compromise or gain unauthorised access to IT, telephony or content, or prevent legitimate access to it.
9. Comply with appropriate policies and guidelines in regard to acceptable usage of IT equipment.

## Personal use of <Organisation> IT

1. Understand that you’re personally accountable for what you do online and with our technology.
2. Ensure that any personal information stored is appropriate. For example, legal, appropriate and compliant with this policy.
3. Ensure that activities do not damage the reputation of our organisation, its employees and clients. These activities include accessing, storing, transmitting or distributing links to material that:
* could embarrass or compromise our organisation in any way
* is obtained in violation of copyright or used in breach of a licence agreement
* can be reasonably considered as harassment of, or insulting to, others
* is offensive, indecent or obscene, including abusive images and literature
1. Follow the <organisation>’s standards of behaviour. Users must not:
* trade or canvass support for any organisation on official premises – whether it’s for personal gain from any transaction or on behalf of external bodies
* send messages or material that solicit or promote religious, political or other causes that are not business-related, unless authorised by our organisation
* provide unauthorised views or commitments that could appear to be on behalf of our organisation
* undertake any form of gaming, lottery or betting
* use any type of applications and/or devices to avoid management or security controls
* download software onto our devices, except when permitted and from an official source that’s appropriately licensed – it must not compromise the performance or security of the device
* access personal webmail accounts on our equipment
* download music, video or other media-related files for non-business purposes, or store such files on network drives

## Email, fax and voice communication

1. Comply with email policies.
2. Only use appropriate language in messages, emails, faxes and recordings. Threatening, derogatory, abusive, indecent, obscene, racist, sexist or otherwise offensive content will not be tolerated.
3. Do not engage in mass transmission of unsolicited emails (spam).
4. Do not alter the content of a third party’s message when forwarding it unless authorised.
5. Try not to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it. For example, through misuse of scanned signatures.
6. Be vigilant to phishing emails and know how to spot and report suspicious emails.
7. Employees and volunteers must not use our email address for personal use. Only use our email address for business-related activities. All employees must use their personal email address for personal activities, including purchasing and selling goods, internet banking and any other personal activity. Failure to comply may lead to disciplinary action.

## Websites and social media

1. Only access appropriate content using our technology and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity, as described in the ‘blocked categories’ list.
2. Contact <role> with requests to block/unblock a website (link is external) and do not attempt to bypass our web filters.
3. Use social media appropriately by making yourselves aware of the ‘Social Media Policy’ and guidelines.
4. Do not put our information, including anything that’s sensitive or personal information, onto online forums, blogs or social networking sites.
5. Only use approved organisation social media accounts for official business and, where appropriate, use our branding and a professional image or persona on the accounts.
6. Be aware that your social media content may be available for anyone to see, which could be indexed by Google and permanently archived.

## Devices, systems and networks

1. Only use systems, applications, software and devices that are approved, procured and configured by our organisation, when undertaking official business.
2. Ensure no official information is stored on devices without our security controls.
3. Raise all software and hardware requests through <role>.

## Physical Security

1. Be responsible for keeping all portable devices assigned to you safe and secure. You must immediately report any loss or damage of your equipment to your line manager and/or the <role>.
2. Protect equipment appropriately when travelling.
3. Never leave a portable device in sight in parked vehicles.
4. Return all equipment when leaving the organisation. The <role> must complete all appropriate exit procedures with leavers.

# Compliance

1. If for any reason users are unable to comply with this policy, they should consult a line manager in the first instance.
2. Line managers are responsible for ensuring that users understand their responsibilities and consequences of their actions, as defined in this policy, and continue to meet its requirements for the duration of their employment. Line managers are also responsible for monitoring employees’ ability to perform assigned security responsibilities.
3. Breaching this policy may result in disciplinary procedures (including possible criminal prosecution) which could lead to dismissal.

# Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this document: annually by the <role>.

Next review date: <date month year>.