
# Acceptable Use Policy

# 1. Purpose

This Acceptable Use Policy (AUP) is intended to provide a framework for the use of Acceleraate assets. It should be interpreted such that it has the widest application to include new technologies which may not be explicitly referred to.

# 2. Scope

This policy applies to all Acceleraate directors, employees, officers, as well as contractors under Acceleraate's direct supervision.

# 3. Acceptable Use

Acceleraate's information processing facilities and systems will be used in accordance with: Specified and published policies, procedures, principles, and guidelines; and all appropriate legislation. This Acceptable Use Policy is approved by and has the full support of the SLT.

## 3.1 Use of Computers, IT Systems and Devices

Acceleraate's computer systems and IT equipment are Acceleraate's property and provided for the benefit of the business. However, colleagues are trusted to use common sense when working with Acceleraate's property and may use these facilities (i.e., computer equipment, laptops, and mobile devices) for private purposes if this is not excessive and does not disrupt their day-to-day work and performance of tasks.

All use of Acceleraate's property, whether business or personal must be appropriate, responsible, and efficient as any misuse or abuse of these systems can have serious legal implications for Acceleraate and may give rise to disciplinary action.

## 3.2 Bring Your Own Device (BYOD)

Acceleraate provides each member of staff with an appropriate computing device, most commonly a laptop of sufficient capability to enable personnel to fulfil their roles.
There are however certain circumstances in which a member of staff may need to use their own personal device. The use of personal mobile devices is permitted, however all devices accessing Acceleraate-owned assets must meet all the criteria of the AUP and any other business policies and procedures.

Related Policies:
BYOD Policy
Mobile Working Policy
Password Policy

## 3.3 Removable Media

The use of removable media is not permitted. Removable media can be defined as, but not be limited to, USB memory sticks, re-writable or single use CDs and DVDs, external Hard Disk Drives (HDDs), Memory cards, such as SD flash memory for mobile phones.

## 3.4 Field Based & Travelling Users

All information processing facilities provided to colleagues will be protected against physical and environmental threats. Sufficient controls will be applied to ensure that equipment is always secured, especially when working remotely or travelling.

Steps to protect portable equipment from theft include:

- Lock devices and information away when not in use.
- If equipment must be left in a vehicle, put it out of view in the boot.
- Consider carrying laptops in something other than a laptop case (for example, many briefcases and small rucksacks are designed to carry a laptop).
- Attempt to keep laptops in sight when it is being security checked at airports.
- Protect mobile devices by a power-on password or PIN, encryption, tracking and remotely manageable (if capable), colleagues shall not disable these settings.
- Use of a privacy screen to shield your screen from onlookers
- Report any faults with any supplied equipment to the appropriate department.
- Report the loss or theft of any mobile device to the appropriate department immediately.
- Where possible mobile devices will have tracking enabled.
- When using portable equipment in public places staff will take care to ensure that confidential information cannot be viewed by unauthorised persons.
- Use of external wireless access points is permitted but staff must ensure that the firewall software provided with the mobile computer is activated.

Related Policies
Mobile Working Policy
Password Policy

## 3.5 Acceptable use of Administration Accounts

Acceleraate operates the principle of Least Privileged Access. It is therefore our practice to provision Standard user accounts for all colleagues. Administration Accounts are controlled solely by IT Services and/or the directors, with password management provided by LastPass, per the Password Policy.

If a colleague requires an Administration Account for the performance of their duties, a Risk Assessment will be completed and any potential workarounds considered, prior to acceptance.

## 3.6 Usernames and Passwords

- All staff are issued with a unique username.
- Single Sign On (SSO) with Multi Factor Authentication (MFA) is mandatory, wherever available.
- Where SSO is not available, MFA remains mandatory, wherever available.
- All default passwords must be changed at the point of first sign-in.
- Acceleraate leverages LastPass for secure password creation and management. All staff are provided with a LastPass account, and this must be used for the creation and management of all passwords.
- If staff believe that their password has been compromised, they must change it immediately and notify their manager.
- Colleagues must not disclose their passwords to anyone, whether inside or outside Acceleraate. If, on occasion, individuals are required to share their passwords with an authorised member of leadership, they must immediately change their passwords once the task is completed.

Related Policies
Password Policy

## 3.7 Clear Screen and Desk

All staff will ensure that the confidentiality of sensitive information is not breached and as such will ensure that their system is protected by a password-enabled screensaver when they are away from their desk. Home screens and common folders must be free of sensitive information. Workplace and desks must be kept secure and tidy by storing any sensitive documents in secure locations.

## 3.8 Information Backup

There is no reason to store information locally on a laptop or computer system. All staff are provided with Microsoft SharePoint and OneDrive storage accounts and all company work and information will be stored here.

## 3.9 Malicious and Mobile Code Control

| | |
|---|---|
| Malware | Malicious software designed to infiltrate a computer system without informed consent. Malware can be hostile, intrusive, and annoying software or program code. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, crimeware, most rootkits, and other malicious and unwanted software. |
| Computer Virus | All types of malwares including true viruses |
| Computer Contaminant | Legal term for malware |

- Acceleraate maintains an up-to-date list of all approved software. Any software which is not on the approved list may not be installed. The process for requesting a new software approval is documented in Notion.
- Staff must always remain vigilant to the threat of malicious software and must never run software or open any files without first ensuring that they are virus free.
- The installation and maintenance of up-to-date anti-malware software on all Acceleraate information systems and devices is mandatory. Staff are responsible for ensuring that their virus definitions are updated on a regular basis.
- The anti-virus/anti-malware software installed on desktops and laptops must not be turned off or its operation disabled.
- Automatic software and operating system updates must be switched on
- Security updates must be installed within 14 days of release
- Autorun/Autoplay functions must be disabled

## 3.10 Protection of Copyright Material

The penalties for breaching copyright are significant. Acceleraate operates a legal software environment and as such colleagues must only use software that supports business processes and is authorised by a director. Staff must not take copies of any company-supplied software nor load any software that is not authorised. The rights of copyright owners (e.g., relating to; software, images, documents, etc.) will be respected.

## 3.11 Internet and Email

Sending and receiving email involves the same responsibilities and approach as would be used when sending or receiving any other form of communication – written or printed mail, fax, telephone call etc. Most users fully understand what would be considered appropriate and acceptable when communicating with others and apply these considerations to their use of email.

**Unacceptable Uses of the Email system include:**

- Use for any unlawful purpose.
- Private business or other for-profit activities not sanctioned by the company directors.
- Seeking to gain unauthorised access to other people's email.
- Harassment of any kind.
- Sending abusive, sexist, racist, homophobic, or defamatory messages.
- Transmission of any copyrighted material in a way that would infringe the rights of the copyright holder.
- Sending, viewing, or storage of pornography.
- Sending messages that aim to, or are likely to, damage the reputation or image of Acceleraate.
- Company email addresses may not be used for personal matters.

Colleagues are prohibited from accessing material that is offensive or subject to legal restrictions. This includes, but not limited to sites that contain pornography, material intended to create unrest, pirated software, etc.

**Unacceptable Uses of the Internet include:**

- Downloading and/or viewing of pornography.
- Criminal activity
- Software or music piracy
- Seeking to gain unauthorised access to the resources on the Internet
- Wasting of resources (people, capacity, computer)
- Alteration or destruction of the integrity of computer-based information
- Compromising the privacy of users or confidentiality of data
- Electronic harassment of any kind

Reasonable personal use of email and the Internet is acceptable, however, abuse of this may result in disciplinary action.

### 3.12 Use of social media for business purposes

Postings (i.e., Social, Blogging, etc.) to sites should contain a disclaimer stating that the opinions expressed are strictly your own and not necessarily those of the company, when posting is related to business duties.

Only authorised chat (e.g., Zoom or Slack) channels should be used in the course of company business. Please refer to the Approved Software list for further details.

Acceleraate expects its staff to refrain from posting about matters relating to politics, or religion on internal and external communication channels from a business perspective.

Related Policies
Social Media Policy

### 3.14 Instant Messaging Services

Utilising Instant Messaging (IM), e.g., Zoom, Slack, WhatsApp is permitted, however, where IM is used, staff must ensure that any information passed over to either other colleagues, or third parties, is in line with the Data Classification Policy and on a need-to-know basis.

### 3.15 Data Protection

Acceleraate is required by law to comply with the Data Protection Act 2018 when processing sensitive personal data. All staff have a personal responsibility to ensure that they make an active contribution towards the company meeting these legal obligations.

### 3.17 Reporting Security Incidents

All staff must report any security incident, weakness, or significant software malfunction at the earliest opportunity via security incident reporting procedures.

### 3.18 Monitoring

Whilst Acceleraate desires to provide a reasonable level of privacy, users should be aware that activity on Acceleraate's systems might be subject to review and monitoring at any time for the purpose of ensuring the security of systems and subject to local laws.

## 4. Policy Review Process

Acceleraate is committed to continually review and improve all of our policies, and may

make changes at any point. At the very least, all policies are reviewed annually and will be issued to all Acceleraate directors, employees, officers, as well as contractors under Acceleraate's direct supervision ("Colleagues").

## 5. Dispensations

In case of any dispensations or deviations from this document please contact the document owner.

## 6. Enforcement & Consequences

Non-conformance or breach by any colleague or third-party members will be subject to investigation and may lead to disciplinary actions, up to and including termination of employment/contract.

Related Policies
Contract of Employment

## Version Control

This is a controlled document produced by Acceleraate Ltd. The control and release of this document is the responsibility of the document owner. This includes any amendment that may be required. This document is ©Acceleraate Ltd, unless otherwise stated.

| # | Change | Date | Author | Approved |
|---|---|---|---|---|
| V1.1 | Document issued | 01.03.23 | Ben Jemison | 01.03.23 |
| V1.2 | Reviewed without changes | 01.03.24 | Ben Jemison | 01.03.24 |

## Document Classification

Public