Acceptable Use Policy (AUP)

Contents

Signed: 

Date: 01.12.25

Review date: 01.11.27

Introduction and aims

The purpose of the policy is to outline the acceptable and unacceptable use of information and communication technology within Integrating.

ICT is integral to the way our organisation operates and is a critical resource for members, staff, Trustees, volunteers and visitors. It supports administrative and pastoral functions of the organisation, as well as enabling communication.

However, ICT can also pose a risk to data protection, online safety and safeguarding.

This policy aims to:

- set guidelines and rules on the use of Integrating's ICT systems, including the database
- establish clear expectations for the way in which everyone engages online
- support Integrating's policies on data protection, online safety and safeguarding
- prevent disruption to the organisation through the misuse, or attempted misuse, of ICT systems
- support staff in the safe and effective use of ICT, websites and social media

Everybody at Integrating has a responsibility to use the organisation's ICT system and database in a professional, lawful, and ethical manner.

All users of Integrating's network should note that it is monitored on a regular basis. Any person who is found to have misused the system or not followed our AUP could face disciplinary action and in the most serious cases, legal action may also be taken.

Legislation and guidance
This policy refers to, and complies with, the following legislation and guidance:

- The General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Searching, screening and confiscation: advice for organisations
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Unacceptable use

Unacceptable use includes:

- using Integrating's IT facilities to breach intellectual property rights or copyright
- using Integrating's IT facilities to bully or harass someone else, or to promote unlawful discrimination
- breaching Integrating's policies or procedures
- any illegal conduct, or statements which are deemed to be advocating illegal activity
- accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- activity which defames or disparages the organisation, or risks bringing the organisation into disrepute
- sharing confidential information about the organisation, its members, or other members of the organisation community
- connecting any device to Integrating's network without approval from authorised personnel
- setting up any software, applications or web services on the organisation's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data
- gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from the Project Manager
- allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to Integrating's IT facilities
- causing intentional damage to IT facilities
- removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel
- causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- using inappropriate or offensive language
- promoting a private business, unless that business is directly related to the organisation

This is not an exhaustive list. Integrating reserves the right to amend this list at any time. The Project Manager and/or Chair of Trustees will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of Integrating's IT facilities.

Sanctions

Staff or members who engage in any of the unacceptable activity listed above may face disciplinary action in line with relevant policies.

In the case of adults who are not staff members, other sanctions are available, such as revoking permission to use Integrating's systems.

Staff are given access to the above policies as part of their induction. This policy is available on our website or on request from the office.

Staff

Access to IT

Individual staff will be provided with unique log-in/account information and passwords to access IT systems. Any changes to this will be at the Project Manager's discretion.

Use of phones and email

Integrating provides staff and Trustees with an email address. This email account should be used for work purposes only.

All work-related business should be conducted using the email address provided by Integrating.

Staff must not share their personal email addresses with parents and members and should not send any work-related materials using their personal email account.

E-mail attachments should only be opened if the source is known and trusted. Spam emails may contain links that can be damaging to IT systems and lead to serious network and equipment hacking.

If required to send an email to more than one recipient, ensure that the email addresses are entered in to the 'bcc' box to ensure that personal email addresses with are not shared with others.

E-mails should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable and public.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

Staff should only use members' first 2 initials when referring to them in written communication e.g Fred Bloggs is FR BL.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Project Manager immediately and follow our data breach procedure.

If for any reason a member of staff feels there is a need to attempt to record a telephone conversation, this should be discussed first with the Project Manager.

Use of printers

There is a main printer in the office at Bullion Hall. This is the printer used for printing documents relating to Integrating and all related matters.

Mobile phone use

Mobile phones are used for essential communication between staff on activities. Staff are allowed to access their personal phones at the start and end of activities to comply with essential administrative tasks for attendance, absence and the management of risk. Mobile phone use during activities is used to share information about the activity and keep in touch with colleagues and or parents/carers, where relevant.

Any photographs/videos of members on activities should be downloaded to the relevant site and removed from personal devices. Staff should not store images of members on personal devices.

Personal social media accounts

Staff should take care to follow the organisation's guidelines on social media use to protect themselves online and avoid compromising their professional integrity.

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Damage to professional reputations can inadvertently be caused by seemingly innocent postings or images.

Staff should **not be** connected to Integrating members and their families on social media unless they are related.

Communication platforms

Staff should consider how they communicate with each other both inside and outside of Integrating when discussing any work matters. This includes during personal time on messaging platforms. Remember that what you may deem as 'personal' messages could unintentionally become public and therefore if organisation matters are being discussed you should consider carefully your use of language and subject matter.

Integrating will always inform staff that any messages relating to the organisation, even in 'personal' forums, should be written carefully and politely and should never contain anything which is likely to cause annoyance, inconvenience or needless

anxiety. Incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Remote access

Staff can access the organisation's IT system remotely through Office 365 and the database on laptops and mobiles.

Staff should ensure they take the necessary precautions to guard against importing viruses or compromising system security.

Our IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

No organisation-related information should be stored on any personal equipment.

If you have a need to work offsite and require electronic or paper-based information to be taken from the organisation, you must:

- Seek permission from the Project Manager for the removal of the information
- Ensure the secure transit of the information
- Ensure that no information is downloaded or stored on personal equipment
- Be aware of other people within the immediate area when viewing personal or sensitive information in areas outside of organisation and limiting such activity away from public places

Integrating social media accounts

Integrating an official Facebook page and all staff are able to post content. The organisation has guidelines for what can and cannot be posted on its social media accounts and staff must ensure they abide by these guidelines at all times. Staff must ensure all members have consent before posting photographs of them onto social media (this information is sought on the annual consent form and can be accessed on the Service Users' profiles on the database).

Images of members

All members need parental permission to have photographs or videos published electronically or in a public area. If in doubt as to whether a member has permission, check with the Team Leader before publishing/displaying. 'Consent to share' information is stored securely on Integrating's database.

No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Images of members must be stored in the designated area of the IT network. It is not permitted to retain images on personal devices. Images should be deleted from electronic devices after uploading to the above storage area.

Members

Access to IT facilities

- Integrating's I-pads and equipment are available to members under the supervision of staff
- Members' use of Discord follows the principles and rules of acceptable use

Search and deletion

Integrating will delete files and data found on searched devices if we believe the data or file has been, or could be, used to break the organisation's rules.

Unacceptable use of IT and the internet outside of organisation

Integrating will sanction members if they engage in any of the following **at any time** (even if they are not on organisation premises):

- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the organisation's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the organisation, or risks bringing the organisation into disrepute
- Sharing confidential information about the organisation, other members, or other members of the organisation community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the organisation's ICT facilities
- Causing intentional damage to IT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Parents

Access to IT facilities and materials

Parents do not have access to the organisation's IT facilities as a matter of course.

However, parents working for, or with, the organisation in an official capacity (for instance, as a volunteer or as a Trustee) may be granted an appropriate level of access or be permitted to use the organisation's facilities at the Project Manager's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the organisation online

We believe it is important to model for members, and help them learn, how to communicate respectfully with, and about, others online.

Parents and staff play a vital role in helping model this behaviour, especially when communicating with the organisation through our website and social media channels.

Monitoring

Integrating reserves the right to monitor the use of its IT facilities and network. This may include:

- Internet sites visited
- Email accounts
- User activity/access logs
- Any other electronic communications

Only authorised staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

Integrating monitors IT use in order to:

- Obtain information related to organisation business
- Investigate compliance with organisation policies, procedures and standards
- Ensure effective organisation and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request (SAR), Freedom of Information Act request, or any other legal obligation

Data security

Integrating takes steps to protect the security of its IT systems but cannot guarantee security. Anybody who uses the organisation's IT facilities should use safe practices at all times.

Passwords

Staff should access IT systems with accounts and passwords as provided. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Anyone who discloses account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Software updates, firewalls and anti-virus software

Integrating's IT systems that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the organisation's IT facilities.

Data protection

All personal data must be processed and stored in line with data protection regulations and Integrating's Data Protection Policy. This ensures any data pertaining to Integrating members and their families, Trustees and staff will be kept private and confidential, except when it is deemed necessary to disclose such information to an appropriate authority.

Access to IT systems

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Project Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use or when they leave the room, to avoid any unauthorised access. Equipment and systems should always be logged out of and closed completely at the end of each working day.

Encryption

Integrating ensures that its devices and systems have an appropriate level of encryption. USB sticks should only be used with the permission of The Project Manager.

Protection from cyber attacks

Integrating will:

- work with Trustees and IT support to make sure cyber security is given the time and resources it needs to make the organisation secure
- provide training for staff at induction, or if new systems are in put in place
- ensure staff are aware of its procedures for reporting and responding to cyber security incidents
- investigate whether our IT software needs updating or replacing to be more secure
- not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- back up critical data on a regular basis on cloud-based backup systems
- ensure each user has the right level of permissions and admin rights
- have a firewall in place that is switched on
- put controls in place that are:
    - **Proportionate**
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the organisation needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are fit for purpose