INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) POLICY

1. Introduction

Esmée Fairbairn Foundation's ("The Foundation's") Information and Communications Technology systems and resources exist as essential business tools. This policy gives guidance on the responsibilities of users to ensure the security, reliability and appropriate use of the systems and resources and its information, data and content.

2. Scope

This policy applies to anyone given access to the Foundation's ICT systems and resources. All employed staff will be deemed to have a contractual obligation to comply with this policy and other users will indicate acceptance of the policy by signing it.

3. Authorised Use

The Network Administrator (Technology Lead or other designated post) will be responsible for enabling authorised use of the ICT systems and resources and monitoring compliance with this policy. The Foundation reserves the right to implement systems for the purpose of monitoring user compliance. The Foundation also reserves the right to restrict access of any user to its ICT systems and resources if it has reason to believe there may be a security breach or misuse of data or systems or any other reason deemed necessary.

4. Personal Use

The Foundation's ICT systems and resources are supplied for business use however reasonable personal use is allowed. Reasonable may be taken as meaning use during lunch breaks or outside normal working hours and must comply with all other aspects of this policy. It must not interfere with your work or availability during working hours. Any and all use of the Foundation's ICT equipment, whether professional or personal, must adhere to the Foundation's wider ICT policy.

5. Security

Users are responsible for the security of their passwords, and any applications accessed via their network account. To maintain security:

- We use a password policy for network access based on password length, uniqueness and lifespan. Passwords must consist of a combination of at least eight letters and numbers. You cannot reuse the last three passwords.
- Common phrases or passwords must not be used. Easily guessable passwords, such as birthdays or the names of loved ones, should also be avoided.
- Users must not reuse passwords across multiple platforms. For example, your password for network access should not be the same one you use to access a social media platform. Staff should make use of the Foundation's approved Password Manager (currently *Lastpass*) to manage this.

- To avoid unauthorised access to your user account, email, etc. you must lock your workstation (*press the Windows and L keys together*) if leaving the workstation unattended.
- Passwords should never be disclosed to colleagues or any other individuals. They should not be written down or stored anywhere in your office, or at home. Passwords must not be stored online, unless it is using the Foundation's approved Password Manager.
- If you suspect that either your password (or a colleague's) may have been compromised, please report this to the Technology Lead and ensure that it is changed immediately. If they are unavailable immediately inform Ramsac the Foundation's ICT support provider.
- Users should not log on to the network using another member of staff's password in order to view network files or emails that are not normally accessible to them or to misrepresent themselves as another network user.
- Passwords to common resources (e.g. logins to news websites) are to be securely stored in the Foundation's approved password manager.

6. Computer Use Procedure

You are asked not to change any workstation or network settings without consulting the Technology Lead. To help with security and effective operation of ICT systems and resources:

- The Foundation uses Microsoft 365 (including OneDrive for Business and SharePoint) to store documents. Users should assume that any documents saved outside of OneDrive or SharePoint, for example documents saved to the desktop, will not be backed up.
- You should not connect your own hardware e.g. phones, memory sticks, cameras, media players, etc. to a networked workstation or laptop without first consulting the Technology Lead.
- Files copied from external hardware should be virus-checked using the Foundation's anti-virus software before copying them to the network. This also applies when using data from a floppy disk, memory stick, CD-ROM or DVD.
- Users should not attempt to unplug or move the hardware facilities provided on the Foundation's premises without first consulting the Technology Lead.

7. Email and Internet Access and usage

You are asked to use the Foundation's email and internet facilities responsibly. Unacceptable use includes:

- Any use which constitutes bullying or harassment on the grounds of gender, race, disability, sexuality or age or any defamatory or fraudulent statement.
- Accessing or distributing pornographic or obscene material.
- Transferring Foundation documents to external third parties without acceptable business reason.
- Deliberately propagating malicious or illegal content.
- Accessing or distributing games, entertainment software or gambling sites or material.
- Any use which may constitute or encourage criminal activities.
- Disclosing information about individuals, which may breach Data Protection Act.
- Disclosing matters confidential to the Foundation without permission.

- Sending chain letters or viruses.
- Using copyrighted information in a way that knowingly violates the copyright.
- Broadcasting unsolicited personal views on social, political, religious, or other non-business-related matters e.g. comment on message boards, discussion sites, chat rooms, instant messaging, etc.
- Making unauthorised commitment for the Foundation to purchase goods or services.
- Use relating to the conduct of a private business or commercial activity.

Internet Browser privacy and security settings must not be changed once set by the Technology Lead.

Caution should be exercised when downloading documents from the internet. Documents, images, toolbars or files without valid security certificates or that infringe copyright laws should not be downloaded to any network folder.

Any attempt to download any software from Internet sites carries a risk of importing a virus and is therefore strictly prohibited. Users who wish to download or purchase **any** new software for use on any system with access to the Foundation must first consult the Technology Lead.

As a general rule if you would not sign your name to a message on Foundation headed paper, **do not** send it by email. Care should be taken to avoid offending or libelling email recipients or other parties, damaging the reputation of the Foundation or breaching the Data Protection Act.

External email messages must contain the name of the user, their official Foundation job title and the Foundation's address. This should be done by setting up an 'auto-signature'.

Messages from unknown senders can potentially contain viruses. As far as possible, the Foundation will filter out any spam or unacceptable emails, however, if you are in any doubt about the contents of an email, please contact the Technology Lead.

Unless you are reasonably sure of the expected contents of a message, **do not open it**. Most "virus" warnings are hoax emails and should be forwarded to the Technology Lead without opening.

The Foundation employs a retention policy on all staff emails. Emails are automatically archived in cloud storage after 36 months and permanently deleted after 7 years.

8. Provision of Laptops by the Foundation

Foundation employees will be provided with a laptop. Staff are advised to abide by the following guidance, in addition to the previous:

- Laptops remain the property of the Foundation, and employees should take every reasonable step to look after them.
- The Foundation can request the laptop back at any point.
- If the laptop is lost, or stolen, it should be reported immediately to the Technology Lead (or Ramsac in their absence).

9. Mobile equipment provided by the Foundation incl. iPhones, iPads

Where appropriate the Foundation may provide mobile equipment (e.g. mobile phones, tablets) to support certain employees in carrying out their roles. Where this is the case, the following guidance is issued:

a) iPhones for SMT staff use

- iPhones are provided primarily to SMT members for business purposes. A reasonable level of personal use is permitted providing it is within the wider guidance provided elsewhere within the ICT policy. If personal use exceeds a reasonable level and incurs additional charges (e.g. excessive data usage or calls abroad), then these costs will be met directly by the employee.
- Handsets/equipment remains the property of the Foundation. Employees should take every reasonable step to look after them. The Foundation can request the handset/equipment back at any time. If the handset/equipment is lost or stolen it should be reported to the Technology Lead immediately.
- Handsets/equipment must always have a passcode, which should not be shared.

b) iPads for staff use

- The Foundation's iPad's remain the property of the Foundation. The Foundation can request their return at any time. iPads are not a contractual benefit.
- The iPad should be used by staff primarily for business use. Reasonable personal use (including downloading applications) is acceptable as long as it falls within the Foundation's wider ICT policy. Esmée retains the right to check content on any device issued.
- Care of the iPad remains the responsibility of the staff member. Should the iPad be lost or stolen the staff member should report it to the Tech Lead as soon as possible.
- All iPad's must always have a passcode which should not be shared.
- Any 'paid for' applications that are for personal use should be paid for by the staff member. Any 'paid for' applications for business use will be uploaded directly by the Technology Lead.

c) Making a business case for an iPhone or iPad

Any request for an iPad must be made to the Chief Operating Officer stating a full business case and confirming agreement to the terms of use.

10. Equipment not provided by the Foundation

- While the Foundation permits the usage of equipment that is not provided by the Foundation (e.g. personal smart phones and tablets.) for work purposes (e.g. accessing emails, calendar, etc.), the Foundation does not take any responsibility for the upkeep, maintenance or support of such equipment nor does it reimburse for any incurred costs.
- If using a personal smartphone for work purposes, the phone must be locked with a passcode or equivalent (e.g. fingerprint or facial recognition).

- Where using a personal device to access Foundation services – e.g. email or Salesforce – only the official apps for each service must be used. For instance, accessing your Foundation email account from your phone's default mail application is not permitted.

11. Using social media

- See our **Social Media Policy** for guidelines for staff on using social media on behalf of the Foundation, and advice for using social media in a professional and personal capacity.

12. Using third party applications, SaaS products, and AI

- Staff must exercise caution and discretion when using any third-party applications, software as a service (SaaS) products, or artificial intelligence (AI) tools. Only those that have been approved by the Foundation should be used. Examples of such tools include cloud storage services (such as Google Drive, or Dropbox), online document editors (including Google Docs), chatbots (including ChatGPT), or data analysis platforms.
- Staff must not share any sensitive, confidential, or personal data with any third-party applications, SaaS products, or AI tools without the prior approval of the Technology Lead and the relevant data owner. Staff must also comply with the Foundation's Data Protection Policy when handling any data.
- Staff must only use third-party applications, SaaS products, or AI tools that have a clear and transparent privacy policy and terms of service, and that adhere to the highest standards of data protection and security.
- Staff must report any incidents or breaches involving third-party applications, SaaS products, or AI tools to the Technology Lead and the Data Protection Officer as soon as possible.

13. Removable Media

- "Removable media" refers to a storage device that can be plugged into a laptop or other computer device, in order to transfer information. This can include USB sticks and external hard drives, as well as CD-ROMs and Floppy Disks.
- Staff are encouraged to determine that there are no other feasible methods of transferring data before using removable media. Alternative forms of transfer may include the use of SharePoint, or email.
- If transferring data via removable media is unavoidable, staff members must request the use of an encrypted USB Stick (via the Technology Lead). Drives are encrypted with Microsoft BitLocker to AES256 standard. Users will be given the password to access the drive for the length of their use. When they are done, the drive will be returned to the Technology Lead, who will securely erase the data, before re-encrypting it with a new passcode.
- There should be very few scenarios where removable media from external sources is required. For most day-to-day file transfer, staff can set up a SharePoint instance, or request the documents be emailed. In both cases, automated systems will scan the files to ensure they are safe. If neither of these are possible, and the staff member must receive the documents via removable media, staff are instructed to first disconnect their workstation from the network, and then scan the removable media using the Windows Defender tool. Once this has passed, they can reconnect to the network.

14. Patch Management

The Foundation operates a variety of hardware, including but not limited to laptops, in order to perform day-to-day duties. This hardware must be kept up to date in order to ensure the performance and security of the Foundation.

- **Laptop Operating System Updates and Patches.** Updates to the Windows Operating System are set to automatically apply in the background when a user is logged in and connected to the internet. Updates are held on a seven day pause, in order to ensure that functionality is not compromised by faulty updates. Staff members must regularly restart their laptops in order to ensure that the latest updates are installed.
- **Laptop Hardware Updates and Patches.** Updates to the Dell Latitude laptops are managed remotely via technology partners Ramsac. Staff members must regularly restart their laptops in order to ensure that the latest updates have been applied correctly.
- **Laptop Antivirus updates and patches.** The Foundation uses Microsoft Defender to protect individual workstations against Malware and other web threats. This software is automatically installed to every workstation and updates are managed centrally and automatically.
- **Updates and Patches to other Office Hardware.** Other office hardware, including the firewall, switches, and wireless access points, are updated by Ramsac during on-site visits every quarter.

Approved by Audit and Risk Committee 10.06.2025