Scottish Funding Council

Acceptable Use Policy

Contents

Introduction

1. The purpose of this policy is to set out the practices that Scottish Funding Council (SFC) staff and other users must agree to on the acceptable use of our Information and Communication Technology (ICT) equipment and services, and to ensure that these equipment and services are used responsibly in line with good practice and legislation.

2. This policy also outlines the acceptable use, security, and management of personally-owned mobile devices (e.g. smartphones, tablets) used to access SFC's resources. The primary purpose is to protect company data while allowing employees the flexibility of using their own devices for work-related tasks.

Ownership

3. All ICT equipment, software and data are the property of SFC unless there is an agreement to the contrary. We reserve the right to monitor and access all information stored or transmitted on it in ways that are consistent with relevant legislation.

4. Examples of our ICT equipment and services include but are not limited to: desktop computers, laptop computers, network servers, Internet service, keyboards, mice, monitors, telephones, voicemail, video conferencing, mobile telephones, PDA devices, SMART devices, network cabling, network equipment, telephone cabling, power cabling, printers, scanners, fax machines, software, electronic file storage, storage devices, tablet devices and storage media.

Scope

5. This policy applies to all permanent and temporary employees, contractors, consultants, secondees, and others who have access to our ICT services. This policy also applies to those individuals who use a personal iOS or Android device to access SFC data using Microsoft 365 apps and services. This policy is to be read in conjunction with SFC's Data Protection Policy and Information Security Policy.

6. For the purposes of this guidance non-SFC managed or personal devices include iOS or Android devices that access SFC data via Microsoft applications and services.

7. Some devices may not have the capability to connect to SFC systems. ICT are not under any obligation to modify SFC systems or otherwise assist staff in connecting their own devices to SFC systems.

General principles

8. You should act in accordance with the following principles.

- Ensure that you treat our ICT services sensibly, responsibly, lawfully, and in ways that are consistent with your duties and with the Council's policies, procedures and values.
- Downloading, copying, possessing and distributing information or other material from the internet or through email may be subject to copyright or other intellectual property rights. If you are uncertain as to the legitimate further use of any data, contact the Information Management and Governance Officer.
- The internet, email and Teams messages are easy and often informal ways of communicating. However, expressions of fact, intention and opinion in an email could be binding legally and may be produced as evidence in court. You should therefore take care when using email, blogs or mailing lists as a means of communication. (In short: THINK before you SEND);
- Downloading, copying, possessing and distributing certain material from the internet or by email may be illegal. Your use of our ICT services for such activities could be subject to disciplinary or legal action, or both. If you are in doubt about information that you are handling, then please take advice from the Information Management and Governance Officer.
- Business information should be treated as confidential and only shared if there is a legitimate reason to do so. Personal information should only be shared where it is compliant with data protection law to do so (See the Data Protection Policy for more information).
- Use of our ICT services should be restricted to business and acceptable non-business use as defined below.
- Users including members of staff should not use SFC systems to store sensitive information for their own personal or non-SFC purposes.
- The contents of SFC systems and SFC data remain SFC's property. This covers all materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages (via Teams) and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for SFC or on its behalf is the property of SFC, regardless of who owns the device.
- SFC data held on personally owned devices is subject to the Freedom of Information Act and the Data Protection Act and must be processed in compliance with information related legislation and associated SFC policies.

- SFC reserves the right to refuse access to particular personally owned devices or software where it considers that there is a security risk to its systems and infrastructure.
- While ICT will always endeavour to assist colleagues wherever possible, SFC cannot take responsibility for supporting non-SFC managed devices.

User Responsibilities when using M365 applications & services on personal devices

9. All individuals who make use of M365 applications and services must take responsibility for their own device and how they use it. They must:

    - Ensure that their iOS device is running version iOS 16 and above or ensure their Android device is running version Android 11 and above before they can be given access to SFC data on personal devices. Ensure they follow the guidance on how to download and set up Microsoft applications 06. Mobile Application Management

    Familiarise themselves with their device and its security features so that they can ensure the safety of SFC information (as well as their own information)

    • Invoke the relevant security features for the device

    • Maintain the device themselves ensuring it is regularly patched and upgraded using updates provided by vendors

    • Ensure that the device is not used for any purpose that would be at odds with SFC'S IT Regulations of Use especially when it is on site or connected to SFC network

    • Pay for their own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs.

10. Staff using M365 applications and services must take all reasonable steps to:

    • Prevent theft and loss of data

    • Keep information confidential where appropriate

    • Maintain the integrity of data and information.

    • Take responsibility for any software they download onto their device.

11. Staff using M365 applications and services must:

    • Set up passwords, passcodes, passkeys or biometric equivalents of sufficient length and complexity for the particular type of device

- Set up remote wipe facilities if available and implement a remote wipe if they lose the device

- Ensure that software on personally owned devices is appropriately licenced

- Encrypt documents or devices as necessary

- Not hold any information that is sensitive, personal, confidential, or of commercial value on personally owned devices. Instead, they should use their device to make use of the facilities provided to access to information securely over the internet.

- Where it is essential that information belonging to SFC is held on a personal device it should be deleted as soon as possible once it is no longer required, including information contained within emails

- Ensure that relevant information is copied back onto SFC systems and manage any potential data integrity issues with existing information

- Report the loss of any device containing SFC data (including email) to the IT Helpdesk

- Be aware of any Data Protection issues and ensure personal data is handled appropriately

- Report any security breach immediately to IT Helpdesk

- Ensure that no SFC information is left on any personal device indefinitely and make sure data is removed before a device is disposed of, sold or transferred to a third party

- Not keep any information longer than is necessary.

12. We expect staff to use our ICT services to support the work of SFC and undertake their duties. However, we also recognise that there are benefits to be gained by allowing staff to make limited personal use of our ICT services. All use of our ICT services should be consistent with this Acceptable Use Policy. To assist with the interpretation of this policy, we define below:

- Business use.
- Acceptable non-business use.
- Prohibited use.

Business use

13. Business use is use required in order for you to do your job, such as accessing and editing documentation, use of email etc. This use allows SFC's activities and

functions to be undertaken effectively, efficiently and in line with our strategies and values.

Acceptable non-business use

14. Acceptable non-business use includes limited personal use of our ICT services for travel, weather, news and current affairs information, internet shopping, internet, social media, banking, personal telephone calls or use of web-based email. Such activities should not interfere with, or take priority over, your work responsibilities.

15. Regarding the personal use of social media, the expectation is that users behave professionally in all situations which relate directly or indirectly to SFC and should conduct themselves in a way which acknowledges the standards of behaviour expected within this and other SFC policies and guidance. This includes the sensible and reasonable personal use of chat rooms, message boards, and mailing lists. Users must ensure that they do not post confidential business or third party personal information on their Social Media profiles.

16. Users must also exercise their judgement in the use of social media – whether or not they explicitly identify themselves with SFC on their personal accounts – to avoid posting material which may cause SFC any reputational damage

17. The time spent accessing, reading or writing web-based e-mail should be reasonably brief or take place during break periods.

18. Subject to bandwidth availability determined by ICT, it is acceptable for employees to stream music from a legitimate source if this will not impede concentration, or disturb co-workers. For the purposes of web monitoring as outlined in the SFC Monitoring Policy, so that we can distinguish between this kind of Internet usage and excessive non-business use, this should be limited to sites which specifically stream music rather than those that offer a mixture of video and music files.

Misuse of ICT systems and facilities

19. The prohibited use of SFC information services, include circumstances where:

    - It is considered offensive or inappropriate by colleagues and visitors in the SFC work setting.
    - It may be unlawful or result in the individual member of staff and/or the Council being liable to legal action.
    - It may damage the reputation of the Council, and/or it is listed as unacceptable use within the JANET acceptable use policy.

- The Chief Information Officer or Assistant Director of ICT shall have the power to remove from SFC's network, any system or facility which is interfering with the operation of the network, or which is being used for purposes which contravene this policy.
- The Chief Information Officer shall have the power to withdraw access to any or all SFC ICT from any member of staff deemed to be in breach of this policy, any applicable legislation or relevant SFC policy, and to require the modification or deletion of personal data to ensure compliance.
- In the event of an apparent breach of this policy by a member of staff, the Chief Information Officer or Assistant Director of ICTs has the authority summarily to withdraw access to the facilities allowed to the staff member.
- Where a member of staff violates this policy, the matter will be dealt with via the Disciplinary Procedures defined by Human Resources and available via their web site.

Examples of 'Prohibited Use'

20. Some examples of prohibited use include:

- Unauthorised or illegal downloading of files or applications (e.g. music, movies, games, pornography).
- Sending emails or storing information with pornographic, gambling or obscene content.
- Visiting or trying to visit pornographic, gambling or obscene websites or websites promoting violence.
- Revealing passwords to colleagues.
- Accessing other colleagues' accounts without authorisation.
- Wilful or intentional damage to our ICT infrastructure; introducing password detecting software or any form of computer virus.
- Accessing or trying to access confidential SFC data for which you have no legitimate business interest (such as HR records).
- Where excessive web browsing or downloading of data and image files impacts significantly on ICT resources, or where there is evidence that it is taking priority over your work responsibilities.
- Introducing unauthorised software or hardware to our ICT infrastructure.
- Sending unsolicited email to business contacts for non-work purposes.
- Excessive personal calls, unauthorised calls to premium rate or overseas numbers, internet telephony.
- Using our ICT services to run a private business.
- Personal downloads such as music (listening is acceptable), movies and games.

21. A prohibited website and offensive material include content of a sexually explicit or sexually oriented nature; material that would offend others on the basis of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation and material relating to illegal or prohibited activities.

22. Where a website is not illegal or expressly prohibited under this policy, but is still decided by the Assistant Director of Human Resources and Organisational Development and the Head of ISU to be inappropriate or offensive, the website will be blocked using web filtering software and this will be communicated to staff, pending any necessary amendments to this policy.

23. Disciplinary and/or legal action may be taken in cases of misuse or prohibited use of our ICT services as set out in out in the Disciplinary Procedure. Gross misconduct in particular may result in dismissal.

Access to user accounts

24. SFC may require access to staff accounts for legitimate business reasons. Where possible, the member of staff will be advised of any access prior to your account being access; however where this is not feasible, SFC may access your account without advising you first.

25. Any access to staff accounts must be authorised by the CEO, a Director or the Assistant Director of HR & OD and must be undertaken in line with the Monitoring Policy. Where it is necessary to gain access to a staff account without notifying the member of staff, this will only be done where it would be disproportionate to contact the individual (for example, if they are on long term sickness absence) or where advising them may compromise an investigation (for example, in the case of an allegation of wrongdoing).

26. SFC may access staff accounts in order to:

    - Access business information which is stored on a user's account.
    - Investigate allegations of criminal or other wrongdoing.
    - To provide IT assistance or maintenance in accordance with the Monitoring Policy

Monitoring and Access

27. We reserve the right to monitor the use of our ICT services, and access any information stored on our ICT infrastructure, in ways that are consistent with relevant legislation and good corporate governance. We will undertake such monitoring to:

    - Comply with our regulatory and statutory obligations.

- Assess compliance with this Acceptable Use Policy.
- Maintain effective ICT systems.
- Prevent and detect unauthorised use or other threats to our ICT system.
- Evaluate staff training.
- Monitor system performance.

28. Such monitoring may include email, internet, telephone, mobile telephone and electronic file storage use. Further details of what we monitor are outlined in the Monitoring Policy.

29. Microsoft 365 introduces its own mobile applications for its suite of services (Microsoft Word, Excel, PowerPoint, Outlook, OneDrive, OneNote, SharePoint, Teams and many more). These can be downloaded from personal devices respective mobile store e.g. Google Play Store. This is called Mobile Application Management (MAM), where in only the corporate apps will be managed by Microsoft Intune. In terms of SFC managing personal phones, only the applications that contain organisational data (SFC) are managed.

30. SFC will not routinely monitor personal devices. However, it does reserve the right to:

    • Prevent access to a particular device from either the wired or wireless networks or both

    • Prevent a device accessing a particular system

    • Take all necessary and appropriate steps to retrieve information owned by SFC.

Compliance

31. All persons identified within the scope of this policy are required to comply with this policy.

Document Control

Title	Acceptable Use Policy
Prepared By	Information Management and Governance Officer
Approved Internally By	Chief Information Officer
Date of Approval	04/12/2023
Review Frequency	Annually
Date of next review	November 2024

Version Control

Version Control	Date	Control Reason	Author
2.0	01/05/2012	General review no change.	-
3.0	09/04/2014	General Review - Changes communicated	-
4.0	27/07/2016	General Review – This policy is now maintained by Corporate Services.	-
5.0	14/08/2018	General review and update for GDPR implementation	C Morrison
6.0	9/11/2023	Update to include MAM and other minor amendments	