Scottish Funding Council

Information Security Policy

Contents

SFC Information Security Policy

Introduction

1. Information security is everyone's responsibility, and all members of staff need to be active in applying and complying with data security guidance and requirements. This policy should be read in conjunction with the Data Protection Policy and Acceptable Use Policy.

2. Failure of SFC staff to comply with this policy may result in disciplinary action. Failure of contractors to comply may result in a breach of contract.

3. If a breach of information security, a line manager, an ISU officer or the Information Management and Governance Officer (IMGO) must be informed immediately.

Physical security

4. Controlling physical access to an organisation's facilities is one of the most important elements of security. The SFC building is kept secure by means of secure car parking area, staffed main reception and, in certain areas, CCTV. The SFC office suites are self-contained with swipe card protected doors.

5. Laptops and other portable electronic devices should be kept secure at all times. Do not leave them unattended and keep them secure outside office hours.

6. Members of staff must:

   - Ensure their SFC pass is carried and visible at all times.
   - Be aware of potential tailgating when entering a secure area, do not assume the person behind you has authorised access.
   - Ensure that visitors and contractors are issued with a pass and are appropriately monitored and escorted at all times.
   - Any person without a pass within the SFC offices, and who you do not recognise as an authorised person, should be politely challenge.
   - Ensure that during office hours unattended areas of the office are kept locked whenever possible.
   - Ensure that any item that provides access to the office or information such as keys, smart cards, ID badges are kept secure at all times.
   - Ensure that your locker is kept locked at all times.
   - Ensure that your desk is left clear of any information when you leave the office.

- ensure that any personal or business confidential information is stored in your locker or in a locked cupboard or cabinet when you are away from your desk
- if you suspect any item that provides access to the office has been lost or stolen, inform your line manager and Data Protection Officer immediately
  If you are concerned with the physical security procedures in your work area, contact either your line manager, a member of ISU or the IMGO

Verbal communication

7. Conversations involving sensitive information should not occur where they can easily be overheard, such as open areas in the office, public places or public transport. Quiet areas or meeting rooms should be used for sensitive information exchange.

Telephone use

8. Telephone conversations involving sensitive information should be conducted discreetly and, where possible, in private. Personal data should not be given out to a caller unless they meet **all** of the following criteria:

   - It is fair and lawful to disclose the personal data.
   - You are satisfied of their identity.
   - It is for a legitimate business purpose.

9. If a member of staff is unsure of any of the above, they should tell the individual that they will get back to them and contact the IMGO for advice.

Emails

10. Use of emails is covered in the Acceptable Use Policy, and the transferring of electronic data is covered in this policy.

11. All staff are required to comply with the following basic security measures when using email:

    - SFC has a firewall and spam filter in place but if you are suspicious of an email or an email attachment do not open it and either use the 'report as spam' function or inform the ISU helpdesk (do not forward the suspicious email).
    - **Never** send business information to your personal email account or anyone else's personal account unless authorised to do so.
    - You may send non-business information to your personal account for your personal convenience – such information may include train ticket bookings or third party newsletters, if you are unsure please consult the IMGO

Never send sensitive personal data by email unless encrypted or authorised to do so. Refer to the section on transfers of data for further guidance

Hardcopy

12. We work in an open plan office so sensitive documents must never be left in plain view as they could easily be viewed or taken by an unauthorised individual.

13. Sensitive or personal information must always be locked away when members of staff are not at their desk.

Fax machines

14. Fax machines should be in kept in secure locations away from public access areas such as reception or windows onto the street.

15. All faxes should be sent with a corporate cover note and contact information. Faxes should be collected immediately they are received and always confirm receipt of fax with the recipient or sender.

Printing

16. Printers should be in secure locations away from public access areas such as reception or windows onto the street.

17. Network printers can only be operated using the owner's smart card or profile password.

18. Key security issues to consider:

    - Do not leave sensitive or personal data printing unattended.
    - Always ensure you take all your printed material with you.
    - Always make sure your print was completed successfully and is not simply waiting for consumables, such as paper or toner, or has a paper jam or other technical fault.
    - Always check the printer before use for previous copy or unfinished print jobs.
    - Double check your own printouts.

Secure disposal: hardcopy and digital

19. Documents that are no longer needed and that contain personal or business information of a sensitive nature should be deposited in the secure confidential waste containers situated around the office. This is mandatory for documents

that contain personal data (other than publicly available business contact information e.g. work email addresses etc.).

20. Where there is uncertainly if the material should be classed as sensitive, caution should be exercised and the information should be disposed of it in the confidential waste bin. For further guidance contact the IMGO.

21. ICT hardware for disposal or recycling must always be with the authorisation and control of ISU.

Digital devices

22. SFC holds most of its information in electronic format on hardware including servers, laptops and mobile phones.

23. Portable devices are convenient, but also present a considerable security risk; staff must be vigilant and mindful of the importance of keeping such equipment safe when away from the office.

24. Many data breach incidents in the UK are the result of loss or theft of ICT equipment. Further guidance for staff working away from the office with ICT equipment can be found in the SFC Remote Working Policy.

Systems security

25. It is the responsibility of ISU to ensure secure firewalls and appropriate anti-virus software is in place and that these are upgraded and maintained regularly.

26. It is also the responsibility of ISU to ensure that disaster and backup procedures are in place and tested appropriately.

27. The electronic systems at SFC rely on user-IDs and passwords for security, so keeping passwords safe is a critical aspect of effective security. The most robust password is alpha-numeric and changed often. See the section on Passwords below for further guidance.

28. Key rules for working with computerised systems including portable devices:

    - Always lock your laptop whenever you leave it unattended, even if just for a short time (press the ⊞ & L at the same time as a shortcut to lock your laptop).
    - Do not keep backup copies of important information on removable storage media such as CDs and flash memory pens – contact ISU if you have additional backup requirements.
    - Do not use your personal email accounts for work purposes. Adhere to the Acceptable Use Policy when using email.

- Always report suspicious or irregular use of an SFC system to ISU.

Passwords

29. Apart from a user-profile password, which enables access to our network, LINKS and Outlook mailboxes, SFC runs various other data systems which are used for finance, statistics and HR, all of which require a robust password policy.

30. Criteria for an SFC password are as follows:

    - Minimum length of 8 characters.
    - Must contain at least one alpha character, one numeric character, and one special character – for example: £, $, *, @, &, etc.
    - The system will remember your three previous passwords.
    - Passwords should be changed every 60 days minimum.
    - You will be locked out after three incorrect attempts to log on.

31. Tips for remembering passwords without writing them down:

    - Use a password based on a mnemonic, such as an easily remembered phrase. For example, take the first letter of each word in a phrase, and then add a few special characters or numbers to it “To be or not to be" can become "2Bor02b?" or replace letters with similar special characters for example an ‘e’ can be replaced with “3” or “£”, an ‘s’ can be replaced with a “$” an so on.
    - Password changes can be simple alterations of the above by using different symbols or additions to the end or beginning of the password, although it is advisable to completely change your password at least once a year
    - If you use multiple systems, then using the same password is acceptable if it is a strong one, but this must be changed regularly.

32. Passwords must never be shared with anyone esle; this includes ISU staff and management. If there is a critical business need to access a member of staff’s work area, for example in the case of absence, this will be done through the proper SFC procedures and not through asking staff for passwords.

33. Passwords must never be written down. If a password is forgotten, ask ISU to reset it.

Transfers of data: electronic data

34. SFC has a secure server for transferring sensitive data from the sectors as agreed in official data sharing agreements. It also has a secure BACS facility. Sensitive personal data or other sensitive business data should never be sent by

email except in exceptional circumstances and ideally must be encrypted. Always seek advice from ISU or the IMGO if planning to send sensitive data by email.

35. If personal data is received without an official data sharing agreement or without encryption, a manager and the IMGO must be informed immediately. Further guidance regarding external data processing can be found in the External Data Processing Policy, or by contacting the IMGO.

Transfers of data: hardcopy

36. Where hardcopy transfers of personal data are necessary, the procedure must be validated and agreed by the IMGO or the Head of ISU in accordance with the External Data Processing Policy.

Data breaches

37. Any data breaches suspected or confirmed must be reported to a line manager and the IMGO immediately. Read the SFC Data Breach procedure for further information.

Contacts

- Information Management and Governance Officer (IMGO): Callum Morrison (Ext: 6566; email: cmorrison@sfc.ac.uk).
- Head of Information Systems Unit: Laurence MacDonald (Ext: 6635; email: Lmacdonald@sfc.ac.uk.
  Assistant Director – Strategy: Richard Hancock (Ext: 6645; email: rhancock@sfc.ac.uk).
- Senior Information Risk Owner (SIRO): Martin Fairbairn (Tel: 6524; email: mfairbairn@sfc.ac.uk).

Document control

Title	SFC Information Security Policy
Prepared By	Information Management and Governance Officer
Approved Internally By	Chief Operating Officer
Date of Approval	20 March 2019
Review Frequency	Annually
Date of Next Review	March 2020

Version control

Version	Date	Control Reason	Author
1	01/07/2010	New version	S. Macauley
1.1	01/07/2011	General review: minor changes	S. Macauley
1.2	01/09/2011	Minor changes regarding hardcopy	S. Macauley
1.3	16/05/2012	Reviewed and amended section on passwords to compliment new robust password system	S. Macauley
1.4	25/05/2012	Reviewed and amended section on printers	S. Macauley
1.4	25/09/2013	No Change	S. Macauley
1.6	21/05/2014	Minor changes to hyperlinks and contact details	S. Macauley
1.7	21/07/2014	Minor re-drafting	Richard Hancock
1.8	01/07/2016	General review: no changes	S. Macauley
2.0	14/08/2018	General review in preparation of GDPR	Callum Morrison