Scottish Funding Council

Remote Working Policy

Contents

Scottish Funding Council Remote Working Policy 1
Contents 2
Remote Working Policy 3
Purpose 3
Health and Safety and working from home 3
Security of data and hardware 3
Cloud Computing: the SFC Extranet, Dropbox, Sharepoint etc. 4
Staff personal ICT equipment 4
Remote working Do's and Don'ts 4
Document Control 6
Version control 6

Remote Working Policy

Purpose

1. This policy provides guidance for Council staff on the safe and correct use of our information and communication technology (ICT) services and devices while working outside the SFC offices.

2. For the purposes of this policy, 'remote working' means any form of working outside of the office. This can mean working at home, in transit, or any other external location, such as hotels, conferences or overseas.

Health and Safety and working from home

3. Under the Health and Safety at Work etc Act 1974, employers have a duty to protect the health, safety and welfare of their employees, including homeworkers. All formal requests to regularly work on a flexible basis – including working from home, or any other non-SFC location – must be agreed through the Council's Flexible Working Requests Procedure.

Security of data and hardware

4. Electronic remote working must only be carried out on SFC equipment or services supplied by ISU. Sending documents or information to your personal (non-SFC) email account and working on local drives on your own PC or laptop is forbidden unless you have special authorisation from the IMGO or SIRO.

5. All members of staff are issued with a laptop to facilitate remote working and should be used for any home or remote working. Some members of staff are provided with mobile phones in addition to laptops to further facilitate remote working.

6. Other ICT data storage and transfer devices belonging to SFC such PDA devices can only be removed from the SFC offices on the authorisation of ISU. An Equipment Loan form is available on the Links homepage. All ICT devices must be returned regularly for anti-virus and data integrity checks as required.

7. SFC Flash pens can be obtained from ISU. These are encrypted but should not be used for storing or transferring large or sensitive personal data sets unless otherwise authorised.

8. All equipment must be secured in a safe and secure place when not being used. ICT equipment or hardcopy containing personal data should be kept in a locked cabinet when in the home or a secure briefcase/laptop case when in transit or overnight travel. Any data storage device or sensitive documents, personal or otherwise should never be left in a car unattended. Hardcopy personal data should only be taken outside of the office if absolutely necessary.

9. All hardware or data losses, thefts or damage must be reported immediately to ISU, the IMGO and HR.

Cloud Computing: the SFC Extranet, Dropbox, Sharepoint etc.

10. External Cloud services such as Dropbox and Google Drive are not to be used for sharing SFC business information. The SFC has an Extranet which has been designed primarily for collaboration with Council members and authorised stakeholders.

11. Please refer to the SFC Acceptable Use Policy and SFC Information Security Policy for further guidance on the use of electronic data sharing or transfers, such as social networking and email usage.

Staff personal ICT equipment

12. Staff should only use their own ICT hardware where authorised by ISU in order to work on virtual gateway software which allows access through a secure link to the Links network. Staff must not transfer SFC documents to local drives on their home computers or unauthorised mobile devices by email or other means.

Remote working Do's and Don'ts

- When in a public place, you must never leave ICT devices unattended.
- Never share your ICT device or data with anyone other than authorised SFC personnel.
- Never allow unauthorised personnel use your accounts.
- Authorised Flash Pens or memory sticks must only be used for anonymous data and never for personal data unless otherwise mentioned.
- Wherever possible, avoid carrying personal data or taking it home.
- Where unavoidable, personal data must be kept to a minimum and removed/deleted from hardware when no longer required.
- Never share personal data with third parties without consent or authorisation from the Information Management and Governance Officer (IMGO) including verbal disclosure or with family members.
- Do not work in a public place such as a train, café, waiting room if you are using sensitive business or personal data.
- When finished with your work, always ensure you log out properly; and switch off your laptop.
- Remember, any information belonging to the Council should be treated as confidential.
- If you do lose any equipment or data inform ISU or the Corporate Governance team immediately.

13. For further information contact:

- Information Management and Governance Officer (IMGO): Emma Pantel (Ext: 6566; email: epantel@sfc.ac.uk).
- Head of Information Systems Unit: Laurence MacDonald (Ext: 6535; email: Lmacdonald@sfc.ac.uk).
- Head of Corporate Governance: Richard Hancock (Ext: 6645; email: rhancock@sfc.ac.uk).

Document Control

Title	ICT Remote Working 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	01/05/2010	General review no change	S. Macauley
1.1	01/05/2011	General review no change	S. Macauley
1.2	01/05/2012	General review no change	S. Macauley
1.3	21/05/2014	Paras 4, and 8, amended to reinforce non-use of personal drives	S. Macauley
1.4	21/07/2014	Minor re-drafting	Richard Hancock
1.5	25/09/2015	Para 6 clarification on use of flash pens. Para 9 Cloud computing, use of the Extranet and future introduction of MS Sharepoint	S. Macauley
1.6	27/07/2016	No changes	S. Macauley
2.0	14/08/2018	Updates to align with GDPR	C. Morrison
2.1	19/03/2021	Minor re-drafting	E.Pantel