Scottish Funding Council

Promoting further and higher education

Scottish Funding Council Data Protection Policy

Document control

Title	SFC Data Protection Policy
Prepared By	Information Management and Security Officer
Approved Internally By	Assistant Director for Learning, Governance and Sustainability
Date of Approval	01-05-09
Review Frequency	Biennially

Version control

Version	Date	Control Reason	Author
1	01-05-10	General review no change	S. Macauley
1	01-05-11	General review no change	S. Macauley
1	01-05-12	General review no change	S. Macauley
1.1	10-09-12	Changes of relevant officer posts and contact names	S. Macauley
1.2	25-03-13	Changes relating to staff photos Paragraph 15	S. Macauley
1.3	25-09-13	Paragraph 11, third bullet changed from Directors to Senior Directors Privacy impact assessments 19-21	S. Macauley
1.3	01-05-14	General review no change	S. Macauley
1.4	21-07-14	Minor re-drafting	Richard Hancock
1.5	20.05.15	General review: minor changes	Alison Kendall
1.6	28-10-15	Post October SFC structure changes. Widening of Privacy Impact Assessment section in preparation for the new DP EU Regulation.	S.Macauley
1.7	27-07-16	Removal of reference to the EU General Data Protection Regulation	S. Macauley

Contents

Introduction

1. In order to fulfil its statutory duties, the SFC needs to hold and process personal information about employees of the Council as well as students and employees of Scotland's colleges and universities. In some circumstances, such as the SFC contact database, we also process the personal data of the general public and other stakeholders. This policy sets out the requirements for processing personal data safely and correctly in accordance with the Data Protection Act 1998 (the DPA) and the eight data protection principles within schedule 1 of the DPA. (See appendix 1 for a list of the data principles).

Accountability at the SFC

2. The Chief Executive (CE) is the Accountable Officer of the SFC and ultimately responsible for the SFC's compliance with the DPA.

3. The Information Management and Security Officer (IMSO) is responsible for annual 'Notification', providing staff awareness training, and the processing of subject access requests. The IMSO also reports to the SFC's Senior Information Risk Owner (SIRO) in matters relating specifically to information security (Principle 7). The SIRO is currently the Assistant Director for Strategy, Richard Hancock.

4. The IMSO will review this policy annually and report to the CE and SIRO with any new statutory requirements or recommendations for amendment.

5. It is also the duty of all staff to comply with the Act. This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the SFC. Any breach of this Data Protection Policy will be treated as a serious matter.

Notification

6. A list of the types of personal data that we process, and the purposes for which we process it, is submitted to the office of the UK Information Commissioner. The Commissioner's office maintains a public register of all personal data processed by UK 'Data Controllers'. This process is called 'Notification'. The SFC's notification reference number is **Z6668573**. To view the SFC's details on the public register go to: https://ico.org.uk/esdwebpages/search

7. Any staff member wishing to process personal data for a purpose other than listed in this notification must first consult with the IMSO or the SIRO.

Definition of personal data

8. Personal data is the information about a living individual that identifies that person. For example, a name accompanied by other information such as address, age, telephone number or information regarding his or her hobbies or financial status. It can be an expression of an opinion about the individual or an indication of the intentions of any person towards that individual. The data can be biographical, even when a combination of different data sources is needed to identify the individual (for example, where individuals are identified only by numbers in a database but a list of to whom the numbers correspond is maintained elsewhere.)

9. Further guidance regarding the definition of personal data can be found on the UK Information Commissioner's website or by contacting the IMSO.

Data Controller

10. A 'Data Controller' is a person or organisation that is responsible for holding and processing personal data and determines for what purpose the data is being processed. The SFC is a data controller under the Act and the CE is therefore ultimately responsible for any personal data we process or contract out to a third party (data processor). The IMSO is the de-facto data controller dealing with day-to-day matters at the SFC.

11. In matters of collaboration and partnership with other bodies, it is possible for either or both organisations to be the data controller, depending upon the nature of the agreement or contract. SFC staff entering into contractual arrangements or collaboration which involves the processing of personal data must first read the SFC External Data Processing Policy and consult with the IMSO or SIRO to consider privacy impact assessments and data sharing agreements before entering into any such collaborations.

Publication of personal information

12. Information that is already in the public domain is generally exempt from the DPA and it is Council policy that the following will normally be available on the SFC website:

- Names of members of staff with work contact details where required

- Names and photographs of Council Board members and SFC directors

- Remuneration details of the CEO, Directors and Council Board members

13. Remuneration details will usually be disclosed where the amount is above the current recommendation for publication of public sector salaries as provided by the Scottish Government (£58,200 as of September 2010). However, disclosure must only refer to staff with seniority and high level decision making powers. The relevant staff may contest processing if this processing is likely to cause substantial damage or substantial distress in accordance with section 10 of the DPA.

14. The SFC internal phone list will not be a public document. However, the telephone extension and email address of staff is available on the SFC website. Any staff member wishing these details or other personal information to be removed from the website where they believe processing is likely to cause substantial damage or substantial distress in accordance with section 10 of the DPA should contact the IMSO.

15. Details or images, either of individuals or small groups, will not normally be displayed on the SFC website or used in other promotional material without the explicit consent of the individuals involved. However, images of large groups at public events, where it would not be practicable to approach each person individually, may be used. Further information and clarification may be obtained from the IMSO.

Staff Photos

16. Staff photos are published internally on the Outlook contacts database. These photos may only be used within emails or other forms of communication with the consent of the staff member obtained by the Communications branch. Copying, pasting transferring, publication or editing of another staff member's photograph, or any other image format, is not permissible unless you are given written consent by the staff member or authorisation by the Head of HR.

Subject Access Requests

17. All individuals (Data Subjects) about whom the SFC holds data, have a right to request access to that information and have it removed or corrected if this information is proved to be in breach of the Data

Protection Principles or is causing distress or damage to the data subject. To make a 'Subject Access Request' if you are a member of staff and wish to see your personal data held by the SFC then contact HR directly. Our 'Access to Information' webpage provides a facility for external individuals to make a request.

Responsibilities of staff and their own data

18. All staff are responsible for:

    - Ensuring that any information that they provide to the Human Resources (HR) team in connection with their employment is accurate and up-to-date
    - Informing HR of any changes to information already provided (for example, new address, bank details etc.)
    - Checking any information that HR sends to them to verify contact and other personal information
    - Notifying HR of any errors or necessary amendments

19. SFC cannot be held responsible for any inaccuracies unless the staff member has previously provided HR with the correct information

Staff responsibilities and data security

20. All staff are responsible for ensuring that they are familiar with and observe the SFC Information Security Policy. With regards to personal data, SFC staff must ensure that:

    - Any personal data which they process is kept securely
    - Personal information is not disclosed either orally or in writing to any third party without appropriate authorisation or written consent of the Data Subject
    - Any new purposes for processing personal data must be subject to a privacy impact assessment
    - Any personal data held electronically is password protected
    - Mobile data storage devices containing personal information are kept securely and in line with our Remote Working Policy

- **Any** breach of personal data must be reported to their line manager or the IMSO immediately. See the Data Breach procedures for further information

21. Unauthorised disclosure of personal data will be considered a serious matter by the SFC management.

Privacy Impact Assessments

22. A Privacy Impact assessment (PIA) is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions to prevent damage or distress for individuals and lessen any risk of financial or reputational damage to the organisation.

23. A PIA should always be carried out in the planning stages when new systems or processes are being considered for the handling of personal data, externally or internally; for example:

24. Implementation of a new HR management database, a contact database, staff surveys and training or new longitudinal surveys). Staff involved with any transfers or external processing must also read the External Data Processing policy. Any staff responsible for such new personal data processing, including policies, systems or databases must contact the Data Protection Officer to assist in completing a PIA. A PIA form is available here on the forms menu of the intranet or by contacting the Data Protection Officer.

25. Detailed information on PIAs can be found on the UK Information Commissioner's website.

Staff awareness and training

26. The Council provides awareness training to ensure that all employees understand their responsibilities regarding the DPA and other aspects of information security at the SFC. This training is provided by the IMSO for all staff and periodically for other staff.

27. For further information on the training programme you should contact the IMSO.

Personal data loss incidents

28. In the event of **any** personal data loss, refer to the Data Breach procedures. The SFC will immediately contact any Data Subject whose data has been lost or compromised and will also inform the UK information Commissioner's office of any personal data breaches.

Misuse and illegal processing of personal data

29. In the event that a member of staff breaches this Policy, an investigation will be undertaken by the SIRO or a senior officer of director rank where necessary. A breach of this Policy may result in disciplinary action and, in some cases, may be considered to be gross misconduct.

30. Staff should note that the UK Information Commissioner has powers to prosecute individuals as well as a corporate body.

31. In all cases of illegal processing of personal data, the UK Information Commissioner and possibly the police will be notified immediately. Illegal use of personal data would include such activities as:

    - Passing on personal data to unauthorised persons for financial gain or otherwise
    - Wilful negligence by failing to follow correct security policies or procedures when processing personal data, especially where this causes distress or damage to the data subject
    - Any instances of unauthorised changes or deletions to personal data which causes distress or damage to the data subject

    This list is not exhaustive.

Further information

32. The UK Information Commissioner's contact details are as follows:

    Information Commissioner
    Wycliffe House
    Water Lane
    Wilmslow
    Cheshire
    SK9 5AF

Tel: 01625 545 745
Fax: 01625 524 510
Email: scotland@ico.org.uk

Website: http://www.ico.org.uk

33. If you have any data protection queries please contact the IMSO.

34. Full contact details of the IMSO and other relevant staff contact links can be found in Appendix 2.

Appendix 1

Data protection principles

35. Schedule 1 of the Data Protection Act 1998 sets out for the proper processing of personal data. The principles state that:

- Personal data must be processed fairly and lawfully
- Personal data must be obtained only for one or more specified and lawful purposes and it must not be processed in a way that is incompatible with that purpose or those purposes
- Personal data must be adequate, relevant and not excessive
- Personal data must be accurate and, where necessary, kept up to date
- Personal data must not be kept for longer than is necessary for its purpose
- Personal data must be processed in accordance with the rights of the data subjects
- Appropriate technical and organisational measures must be taken against accidental loss, destruction and damage to personal data
- Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data

Appendix 2

Key contacts list

Job title	Name	Telephone number	Email address
Information Management and Security Officer (IMSO)	Simon Macauley	0131 313 6569	smacauley@sfc.ac.uk
Senior Information Risk Owner (SIRO) and Assistant Director Corporate Services	Richard Hancock	0131 313 6645	rhancock@sfc.ac.uk
Head of Information Systems Unit	Laurence McDonald	0131 313 6535	lmcdonald@sfc.ac.uk
Head of Human Resources	Ian McCracken	0131 313 6597	imcracken@sfc.ac.uk