# Scottish Funding Council

Data Protection Policy

## Contents

## Introduction

1. The Scottish Funding Council (SFC) processes personal data in order to carry out its statutory functions, and to promote and improve further and higher education in Scotland.

2. SFC is committed to processing personal data in line with Data Protection Legislation and specifically in line with the Data Protection Principles as outlined in Appendix A of this policy.

3. SFC will process personal data in accordance with guidance from the Information Commissioner's Office (ICO)[1] and the European Data Protection Board (EDPB).[2]

4. For the purposes of this policy, Data Protection Legislation will collectively refer to:

   - General Data Protection Regulation (EU) 2016/679 (GDPR)
   - Data Protection Act (UK) 2018 (DPA)
   - Privacy and Electronic Communication Regulation (EU) 2002/58/EC (PECR)

## Policy Review

5. The Information Management and Governance (IMGO) will review this policy annually and report to the Chief Executive and Chief Operating Officer (in his capacity as Senior Information Risk Owner) with any new statutory requirements or recommendations for amendment.

## Registration

6. The Scottish Funding Council is registered as a Data Controller with the Information Commissioner's Office with the registration number Z6668573.

## Accountability at the SFC

7. The Chief Executive (CE) is the Accountable Officer of the SFC and ultimately responsible for the SFC's compliance with data protection legislation.

8. The Information Management and Governance Officer is the assigned Data Protection Officer (DPO) for the Scottish Funding Council. The

[1] The ICO is the UK's independent body set up to uphold information rights
[2] The EDPB is an independent European body established under the GDPR, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.

responsibilities of the Data Protection Officer are described in paragraphs 22-24 this policy.

9. The SIRO is responsible for management decisions concerning data protection and for ensuring that data protection issues are given due consideration at senior management level.

10. It is the duty of all staff to comply with Data Protection Legislation. 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 and may result in disciplinary action.

**Definition of personal data**

11. Personal data is any information about a living individual.

12. Data is considered personal data even if it identifies a living individual indirectly. The data does not necessarily need an individual's name or other single unique identifier to be considered personal data.

13. For example, if we hold data on a student which identifies the course they are on, their gender and date of birth; it is likely that this would be personal data even though no one of these categories would identify the individual in isolation.

14. Further guidance regarding the definition of personal data can be found on the Information Commissioner's website Members of staff should consult with the IMGO if they are unsure if data is considered personal data.

**Special category personal data**

15. Special category personal data is a subcategory of personal data defined in data protection law that requires additional protection.

16. Special category data is any personal data that relates to an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;

- sex life; or
- sexual orientation.

17. This Policy acts as the *Appropriate Policy Document* as required by paragraph 39 of Schedule one of the Data Protection Act 2018 for processing special category data.

**Definition of a Data Controller**

18. A 'Data Controller' is an organisation or occasionally a person that is responsible for processing personal data and determines means and purposes for processing that data. SFC is a data controller and we are responsible for any data we process or contract out to a third party (data processor).

19. SFC is also a joint controller for some of the data we hold meaning we are jointly responsible for it at different stages of its lifecycle.

**Data Sharing**

20. When SFC shares or collects personal data with another organisation, it must be do so in line with our External Data Processing Policy. When sharing or collecting personal data, the IMGO should be consulted to consider if a Data Protection Impact Assessment needs to be completed prior to the data sharing.

21. Personal data should not be transferred outside of the European Economic Area unless appropriate safeguards are in place. Members of staff must consult the IMGO prior to any international transfers of personal data, including the use of cloud storage.

**Record of personal data processing**

22. SFC must record what personal data we process. This record must include the following information for each data set:

    - Contact details for SFC.
    - Name and contact details of the DPO.
    - Purposes of processing.
    - A description of the categories of the data subjects and categories of personal data.
    - If the data is transferred to a country outside of the UK or EU (including by electronic cloud storage.)
    - Where possible the retention periods for the data.
    - Where possible a general description of the technical and organisational security measures in place.

23. The IMGO will be responsible for maintaining the records of processing in consultation with other members of staff.

24. Any member of staff wishing to process personal data not listed in the records of processing, or wishing to process any of these data for a different purpose, must first consult with the IMGO.

**Data Protection Officer**

25. As a public body, SFC is required to appoint a Data Protection Officer. The role of the DPO is governed by the GDPR and the DPA.

26. In line with GDPR requirements, the tasks of the Data Protection Officer are to:

- Inform and advise SFC of their obligations under Data Protection Legislation.
- Monitor SFC's compliance with Data Protection Legislation and associated data protection policies (as described in the Information Management Framework).
- Raise awareness and ensure adequate training is in place for members of staff.
- Cooperate with the Information Commissioner's Office (ICO) on behalf of SFC.
- Act as a point of contact for the ICO on issues relating to the processing of personal data including prior consultation where required.
- Have due regard for the risks associated with the processing of personal data at SFC.
- Act as a point of contact for data subjects in regards to the processing of their personal data.

27.

28. In line with GDPR requirements, SFC shall ensure that the Data Protection Officer is:

- Involved properly and in a timely manner in all issues which relate to the protection of personal data.
- Provided with support in carrying out their tasks providing the necessary resources, access to personal data and processing operations and to maintain their expert knowledge through appropriate training.
- Not dismissed or penalised for performing their tasks as DPO.
- Able to report to the senior management team and board on matters concerning data protection when required.

- Not asked to undertake any additional tasks which would result in a conflict of interest with the role as data protection officer.
- Able to carry out their tasks in an independent manner.

**Data Protection Impact Assessments (DPIA)**

29. A DPIA helps SFC assess data protection risks for new projects involving the use of personal data

30. It is a legal requirement for SFC to carry out a DPIA when there the processing of data is likely to result in a 'high risk' to the data subjects. SFC policy is that an initial assessment must be carried out for any project involving personal data, even if it is decided that a full DPIA is not needed.

31. A DPIA should be completed in line with SFCs separate DPIA template and Guidance.

**Data Retention**

32. SFC shall ensure that all personal data is only kept for as long as is necessary.

33. SFC's Retention Schedule shall include appropriate retention periods for all personal data processed by the organisation.

**Information Security**

34. All personal data must be processed in accordance with the SFC Information Security Policy including, but not limited to, ensuring that:

    - Any personal data which is held is kept securely.
    - Personal information is not disclosed either orally or in writing to any third party without an appropriate agreement in place or the consent of the individual.
    - 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 the Data Protection Officer immediately. See the Data Security Incident Procedure for further information.

35. Unauthorised disclosure of personal data will be considered a serious matter by the SFC management and may lead to disciplinary action.

**Data Subject Rights**

36. The GDPR provides data subjects (i.e. individuals who we hold personal data about) with a number of rights in relation to their personal data.

37. SFC is committed to upholding data subject's rights. However, it should be noted that most of SFC's data processing is on the basis of fulfilling its statutory functions, and therefore some of these rights will only apply in limited circumstances as described below.

38. To assist data subjects in exercising their data subject rights we have developed a template form included in appendix C.

***The right to be informed***

39. Data Subjects have a right to be informed about how SFC uses their personal data. To achieve this SFC will publish privacy statements on its website that cover the processing of all personal data except that of SFC staff.

40. Privacy notices for SFC staff will be provided internally and proactively communicated to staff.

41. Where we collect personal information directly from data subjects, we will communicate how we intend to use this information to them at the point of collection.

***The right of access***

42. Individuals have the right to request access to the data that SFC holds about them; this is known as a Subject Access Request.

43. The GDPR also provides that the Data Subject can request to know the purposes of processing their personal data, the categories of personal data that are processed, who their data is shared with, how long the data is retained for, what other rights they have in relation to their data, and weather SFC uses their personal data to make automated decisions.

44. SFC will respond to these requests as soon as possible and no later than one calendar month from the date of receipt.

***The right of rectification***

45. If SFC holds any incorrect personal data, the Data Subject has the right to have any personal data corrected without undue delay.

46. The right to rectification also applies where SFC hold incomplete data. The Data Subject will have the right to have that personal data completed in this instance.

***The right of erasure***

47. Data Subjects will also have the right to erasure, often referred to as the 'right to be forgotten' if one of the following circumstances apply, subject to the conditions of the GDPR:

    - It is no longer necessary for SFC to process the data for the established purposes; or
    - The data was processed on the basis of consent and the data subject withdraws their consent; or
    - The data subject has objected to SFC processing their personal data and there are no overriding legitimate grounds in line with the GDPR; or
    - The personal data has been unlawfully processed; or
    - The personal data have to be erased for compliance with a legal obligation on SFC.

***The right to restrict processing***

48. If the personal data that SFC processes is inaccurate, unlawful or is no longer needed for established purposes, a Data Subject can request that SFC's processing of their personal data is restricted only to the holding of their personal data.

49. Any further processing shall only be with the consent of the Data Subject where this applies

***The right to object***

50. Where SFC carries out processing on the basis of the processing being necessary for the performance of a task in the public interest, or in order to pursue legitimate interests, Data Subjects have the right to object to their data being processed.

51. When such an objection is received, SFC will stop processing this data unless we can demonstrate compelling legitimate or public interest in continuing the processing.

***Rights related to automated decision making and profiling***

52. SFC does not carry out any profiling or make decisions about Data Subjects on a solely automated basis using their personal data.

53. Rights in relation to profiling and automated decision making therefore do not apply.

**Staff awareness and training**

54. SFC will ensure that members of staff are adequately trained on data protection legislation and practice.

55. Staff will be trained on joining the organisation and will be offered refresher training annually or if there is a significant change to the legislative environment. Members of staff must complete training at minimum intervals of every two years.

56. Training will be relevant to the data processing which members of staff carry out.

**Personal data incidents**

57. The Data Protection Officer (IMGO) must be contacted immediately in the case of any loss or unauthorised access, destruction or disclosure of personal data.

58. The Data Security Incident Procedure must be followed in the case of a personal data incident.

**Misuse and illegal processing of personal data**

59. In the event that a member of staff breaches this Policy, an investigation will be undertaken in line with the Data Security Incident Procedure. A breach of this Policy may result in disciplinary action and, in some cases, may be considered to be gross misconduct.

60. Staff should note that the UK Information Commissioner has powers to prosecute individual members of staff, as well as SFC as a corporate body, for the misuse of personal data

61. In all cases of personal data being used for illegal purposes, the UK Information Commissioner and possibly the police will be notified immediately. Illegal use of personal data includes but is not limited to activities such as:

    - Passing on personal data to unauthorised persons for personal or financial gain.
    - 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.

- Using personal data provided to members of staff to carry out their job for your own purposes outside of work.

**Further information**

62. The UK Information Commissioner's (Scotland Office) contact details are as follows:

    Information Commissioner
    Wycliffe House
    Water Lane
    Wilmslow
    Cheshire
    SK9 5AF

    Tel: 0303 123 1115
    Email: scotland@ico.org.uk

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

63. If you have any data protection queries please contact the IMGO.

64. Full contact details of the IMGO and other relevant staff contact links can be found in Appendix B.

**Document control**

| | |
|---|---|
| **Title** | Data Protection 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 | 10/09/2012 | Changes of relevant officer posts and contact names | S. Macauley |
| 1.2 | 25/03/2013 | Changes relating to staff photos Paragraph 15 | S. Macauley |
| 1.3 | 25/09/2013 | Paragraph 11, third bullet changed from Directors to Senior Directors Privacy impact assessments 19-21 | S. Macauley |
| 1.3 | 01/05/2014 | General review no change | S. Macauley |
| 1.4 | 21/07/2014 | Minor re-drafting | Richard Hancock |
| 1.5 | 20/05/2015 | General review: minor changes | Alison Kendall |
| 1.6 | 28/10/2015 | Post October SFC structure changes. Widening of Privacy Impact Assessment section in preparation for the new DP EU Regulation. | S. Macauley |
| 1.7 | 17/07/2016 | Reference to the EU General Data Protection Regulation | S. Macauley |
| 1.8 | 21/07/2017 | General review and update on GDPR | Sheila Meehan |
| 2.0 | 14/08/2018 | Updated with full GDPR requirements. Reframed as a high | Callum Morrison |

| | | | |
|---|---|---|---|
| | | level policy removing references to operational decisions. | |

## Appendix A: Data protection principles

Article 5 of the General Data Protection Regulation sets out the Data Protection Principles, these principles must be adhered to when processing personal data.

**Lawful, Fair and Transparent**

- SFC must have a legal bases as set out in data protection law to process personal data.
- SFC must ensure that its processing is fair with due regard to the rights of the data subjects.
- SFC must be transparent in processing personal data by communicating how personal data is used.

**Purpose limitation**

- SFC must collect personal data for specified purposes.
- SFC must only use personal data for those specified purposes.

**Data Minimisation**

- SFC must only collect the minimum amount of personal data necessary to carry out those purposes.
- Any personal data which is no longer necessary should be destroyed.

**Data Accuracy**

- SFC must ensure that personal data is kept accurate and up to date.
- Any inaccuracies in the personal data that SFC holds must be corrected.

**Data Retention**

- SFC must ensure that personal data is not kept for longer than is necessary for those purposes.
- Personal data kept for statistical purposes must be anonymised wherever possible.

**Data Security**

- SFC must ensure that personal data is kept securely.
- SFC must take appropriate technical and organisationa.l measures to ensure the security of personal data it processes.

The GDPR also requires SFC to be able to demonstrate compliance with the principles, this is sometimes referred to as the “accountability principle”.

## Appendix B: Key contacts list

65.

| Job title | Name | Telephone number | Email address |
|---|---|---|---|
| Data Protection Officer (DPO) and Information Management and Governance Officer (IMGO) | Emma Pantel | 0131 313 6566 | epantel@sfc.ac.uk |
| Senior Information Risk Owner (SIRO) and Chief Operating Officer | | | |
| 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 |

## Appendix C: Data Rights Form

Data protection legislation gives individuals (data subjects) rights regarding the use of their information including to obtain copies of information held about themselves (exemptions may apply). SFC must respond to such a request within one calendar month from the date of the request

SFC may request satisfactory proof of your identity prior to processing your request. The level of identity evidence required will depend on SFC's relationship with the data subject and the sensitivity of the data requested. The time limit for SFC's response will not start until we have appropriate proof of identity.

**Personal Details**

To process your request we ask that you fill in this form providing all relevant detail to allow us to accurately identify and provide copies information which relates to you. We use the data that you provide in this request for the explicit purpose of processing your access request. For more information on how we use your personal data please see our Privacy Notice.

Please only provide information which is necessary for us to carry out your request, Fields marked with an asterisk (*) are considered necessary in all cases.

| | |
|---|---|
| **Title (Mrs/Mr/Miss/Dr etc)** | |
| **Surname/Family Name*** | |
| **First Name(s)*** | |
| **Former/Maiden Names** | |
| **Address** | |
| **Post Code** | |
| **Previous addresses** | |
| **Telephone Number and/or email address** | |
| **Preferred format of information** | |

| | |
|---|---|
| **(electronic, paper, in person)*** | |
| **Scope of your request. Please provide as much detail as possible about which right you wish to exercise and the information this relates to.**<br><br>**For example, in the case of an access request consider the information you wish to access such as:**<br>• **Your relationship with SFC (i.e. an ex member of staff or a student whose data we may hold)**<br>• **Relevant date range of the information**<br>• **Specific types of information you are interested in**<br><br>**In the case of an objection, restriction or erasure request, please advise us of what grounds you wish SFC to limit/stop processing your personal data.** | |

**Declaration**

Statement 2 is to be used where an agent is acting for the data subject.

1. The information which I have supplied in the application is correct and I am the person to whom it relates[3]

Signed _____ Date _____

Please send this form to:

Information Management and Governance Officer
Scottish Funding Council
Donaldson House
97 Haymarket Terrace

[3] If you are requesting the personal data of another individual, we will need to obtain their explicit consent for you to conduct the request on their behalf

Edinburgh
EH12 5HD

Email: info@sfc.ac.uk

If you require any assistance completing this form, or would like any further information, contact us using the email address above, or Tel: 0131 313 6566.