Scottish Funding Council

Promoting further and higher education

External Data Processing Policy

Document control

Title	External Data Processing 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	Minor changes to hyperlinks and job titles	S. Macauley
1.2	24-09-13	Changes referring to need for PIA's. Para 4.	S. Macauley
1.3	21-05-14	Slight change to PIA para, heading added.	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	20-07-16	General review – minor changes	Simon Macauley

Contents

External Data Processing Policy

Purpose

1. This policy sets out our procedures for the safe handling of personal data that is processed on our behalf by external agents (Data Processors). Scottish Funding Council (SFC) staff should follow this policy when commissioning any external data processing services.

Policy statement

2. The SFC Data Protection Policy commits SFC to processing personal data in accordance with the eight principles of the Data Protection Act 1998 (the Act). As a 'Data Controller', we will not process any personal data without the data subject's consent, except where the Act enables processing (for example, to comply with a court request).

3. External data processing services commissioned by SFC must comply fully with our terms and conditions regarding data security and will be regularly monitored to ensure compliance with the Act and ISO/IEC 27001:2005 (or any replacement standard relating to data security).

Privacy Impact Assessments

4. A Privacy Impact Assessment (PIA) must always be carried out where there is any new or modified processing of personal data on behalf of the SFC. Please refer to the SFC Data Protection Policy for guidance regarding PIAs.

Tendering and procuring of external processing services

5. Staff who are involved with procurement and tendering of goods and services which may involve the processing of personal data for any purpose including, but not limited to, student or staff surveys; equalities monitoring; or performance monitoring, must first consult with the Information Management and Security Officer (IMSO).

6. The IMSO is the 'Information Asset Officer' (IAO) and the 'Data Security Officer' (DSO) for SFC. The IMSO is also the 'Data Protection Officer'.

7. The IMSO must also be consulted:

    - If re-drafting of the SFC terms and conditions for ICT services, professional services or goods and related is required

    - When any new SFC terms and conditions for external services are being drafted

- When re-drafting of the SFC tendering process is required
- When the contracted Data Processor employs a new sub-contractor
- Immediately if any data protection issues arise with a data processor or sub-contractor (for example, loss of data, a breach of the Act, or complaints from data subjects)

Data Processors

8. 'Data Processors' are external agencies or persons commissioned by, or acting on behalf of, a 'Data Controller' (the SFC is the Data Controller in this instance). A typical Data Processor would be an agency or consultant commissioned by the SFC to carry out a student or staff survey or statistical analysis. Sub-contactors commissioned by the contractor are also Data Processors according to the Act. Therefore, as Data Controller, SFC is also responsible for any processing carried out by the sub-contractor.

9. SFC must ensure any sub-contracting is carried out with our full knowledge and agreement. SFC must have sight of, and agree to the suitability of, any contract between the contractor and sub-contractor with regards to data protection and data security.

Large data processing exercises

10. Where external processing of a broad and deep personal dataset is to be commissioned, then the UK Information Commissioner's Scottish office (ICO) must be consulted first. An example of such a processing exercise would be where personal data is being processed for more than a 12 month period and involves students or teaching staff.

11. If any directorate is planning such an exercise they must first contact the IMSO. Where appropriate, the IMSO will facilitate a meeting with the ICO in Scotland and the project leader to ensure the survey is safe and robust and meets the requirements of the Data Protection Act 1998.

Data transfers between SFC and Data Processors

Electronic transfers:

12. Electronic transfers of personal data from and to SFC and between Data Processors must be securely encrypted. Integrity of electronic methods of data transfer between Data Processors, or between a Data Processor and SFC, must be agreed to by the IMSO and the Head of ISU at the beginning of a contract or when and as changes in procedure or contract are made. The IMSO must be informed immediately by the Data Processor of any such changes.

13. SFC currently uses a secure server for the majority of data transfers (personal or anonymous). Wherever possible, staff should use this facility for external transfers of personal data with contractors and Data Processors. Contact the IMSO or the Head of ISU for further information.

14. Emails between SFC and Data Processors, which contain personal data should only be sent in exceptional circumstances and must be encrypted. If personal data is received without encryption you must inform your line manager and the IMSO immediately.

15. Guidance on encryption and validation methods can be obtained from ISU or the Corporate Governance team. The IMSO or the Head of ISU must be consulted before any new data transfer agreements and procedures are implemented at SFC.

16. Any breaches of data security or data loss must be reported to your line manager and the IMSO immediately. Please read the guidance on SFC Data Breach Incident Procedures.

Hardcopy transfers

17. External transfers of personal data in hardcopy have been the cause of many data loss incidents within the UK public sector. To mitigate against such events occurring at SFC, hardcopy transfers must only be carried out where absolutely necessary and only then using the strictest and most secure methods available.

18. Points to consider when transferring personal data in hardcopy :

    - Always consider whether personal identification data needs to be transferred in this way at all

    - Where it is practical, consider anonymising the personal identification data before transfer

    - If possible, separate personal identification data from the rest of the data and send each part separately

19. Where hardcopy transfers are necessary, the procedure must be validated and agreed by the IMSO or the Head of ISU at the beginning of a contract and if any changes are made to the procedure.

20. Appropriate methods of transfer would be:

    - Transfers of personal data must be on a 'point-to-point' basis. This means transferring the information directly from one processor of data to another. This must be done using a secure, well-established and

recognised courier service or by vehicles owned by the Data Processor and driven by their staff.

- Non personal or anonymised data must be transferred using a secure, well-established and recognised courier service.

21. All transfers of data must be recorded and signed for by a senior manager.

22. The IMSO or the Head of ISU must be informed of any new or ad hoc transfers of personal data into, or externally from, SFC.

Further Information

23. For guidance or advice on this policy contact the IMSO, Simon Macauley (telephone: 6691; email: smacauley@sfc.ac.uk).