Skills Development Scotland

# Data Protection Policy

## Introduction

This policy sets out the framework for a consistent SDS wide approach to handling information relating to identifiable individuals (Personal Data). Skills Development Scotland stores and processes personal information on behalf of its clients, partners and employees and has a duty to protect the information as mandated by the Data Protection Act 1998.

## Purpose

1. The purpose of the Data Protection Act 1998 is the protection of the individual from having his/her personal data or privacy exploited or abused. This places the onus upon organisations and individuals processing such data to ensure that the processing is conducted in a fair, lawful and secure way. It is therefore of vital importance that all SDS employees comply with the requirements of the Act.

2. SDS is committed to adopting best practice in protecting the personal information of all its customers, staff, consultants and contractors and also employees of partner and supplier organisations. This policy sets out the approach adopted by SDS to comply with the legal requirements and maintain the trust of customers, partners and employees.

3. The main provisions of the Data Protection Act 1998, including the eight Data Protection Principles, are included in Appendix 1.

## Scope

4. This policy applies to all employees including temporary and seconded individuals.

5. Breach of this policy may be dealt with under our Disciplinary Policy and Procedure. Any member of staff who does not comply with the Act either deliberately, recklessly or by neglect could face criminal prosecution.

## Definitions

6. The following key concepts need to be understood:

   - *Personal Data* – is information held about living, identifiable individuals, including expressions of opinion or intention about them;
   - *Data Controller* – an organisation or individual who controls the contents and use of personal data;
   - *Data Processor* – a person or organisation who processes data on behalf of a data controller e.g. payroll bureau;
   - *Data Subjects* – are individuals about whom the data is held; and

- *Processing* – obtaining, recording or using the data, including organisation, adaptation, alteration, retrieval, disclosure, or erasure of it or any combination of these.

## Relevance to SDS

7. The Act covers all information about living individuals. For SDS this covers:

   - Clients (young persons, users of our services);
   - Employees and ex-employees of SDS and its predecessor companies; and
   - Partners/Suppliers (information about directors, partners, sole traders or employees of the company or organisation is covered, including contact details).

## Notification

8. All Data Controllers are required to notify their processing to the Information Commissioner. Notification is a formal process which involves specifying the purposes for which data is processed, the classes of data subject and data items and the classes of parties to whom the information may be disclosed. Standard lists of purposes, data subjects, data classes and recipients are provided. The Register of Data Controllers is available for public inspection on the internet at:

   http://www.ico.gov.uk/Home/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

9. SDS's notification covers the following purposes:

   - Accounts and Records;
   - Staff Administration;
   - Advertising, Marketing and Public Relations;
   - Benefits, Grants and Loans Administration;
   - Consultancy and Advisory Services;
   - Education;
   - Information and Databank Administration;
   - Research; and
   - Crime Prevention and Prosecution of Offenders (this relates to our use of CCTV for security purposes).

## Roles and Responsibilities

10. The ***Information Governance Leadership Group*** are responsible for ensuring appropriate co-ordination and oversight is in place to ensure that SDS remains compliant with the Data Protection Act. The group commissions and approves Data Protection policies and procedures.

11. The ***EIS Information Assurance Team*** is responsible for development and publication of Data Protection policies and procedures and for providing guidance on compliance in straightforward cases.

12. The ***EIS Information Manager*** is responsible for the Data Sharing Policy and providing guidance and assistance on data sharing. The EIS Information Manager maintains the register of active data sharing agreements and is also the Data Protection Officer responsible for SDS's DPA notification and the Data Protection Policy.

13. ***The SDS Legal Team*** are responsible for providing guidance on the interpretation of the Act in more complex cases and where there are issues around the interface of the DPA and other legislation.

14. ***Information Asset Owners*** must ensure that personal data is only processed and disclosed under the terms of the notification, and that any new purposes for which personal data is processed or new classes of data subject or parties to whom disclosure will be made are notified to the Data Protection Officer for inclusion in an updated notification. Information Asset Owners will engage with EIS to identify measures required on IS systems to protect their information. Information Asset Owners are also required to co-ordinate and monitor compliance with Data Sharing Agreements.

15. ***Information Coordinators*** are staff nominated within each business unit to handle both DPA and FOI information requests. They are responsible for ensuring requests are dealt with according to the required timescales and for updating the register of requests held by the Corporate Office.

16. ***People Managers*** are responsible for ensuring that access to personal data is granted to their staff in accordance with their duties. Staff are made aware of the Data Protection Policy and provided with appropriate training and guidance as required, with input from the Data Protection Officer and/or Corporate Office as appropriate.

17. ***All Employees*** are responsible for ensuring that they understand the implications of the Act and the Policy for their roles, and comply.

18. ***Human Resources*** are responsible for co-ordinating the response to Subject Access Requests where the requester is an employee or former employee.

19. ***Enterprise Information Services*** are responsible, along with system owners, for ensuring adequate security is in place to protect personal data held on computer systems.

20. ***Facilities Management*** are responsible for ensuring adequate secure storage is available for personal data in hard copy.

## Compliance Requirements – All Employees

21. The following guidance applies to all staff in relation to any processing of personal information which they undertake.

22. It is important that the person to whom the personal information relates to is aware of the following:
    - Why we need it; ask only for what we need and not collect too much or irrelevant information;
    - Protect it and make sure no unauthorised person has access to it;
    - Let the data subject know if we will share it with other organisations and give them the opportunity to refuse;
    - Make sure we don't keep it any longer than is necessary;
    - Not make the data subjects personal information available for commercial use without their consent; and
    - Consider the data subjects request to stop processing data about them.

23. Obtain sufficient data for the purpose.

24. Where items of personal data would be useful to us, but are not essential, obtain the data subject's consent or ensure that they are aware they have a choice about whether to provide them.

25. Do not collect excessive items of personal data on the basis that they might be useful for some unspecified purpose in the future.

26. Obtain or accept data only from sources which are lawfully allowed to supply it.

27. Disclose the data only to parties who require it in relation to the purpose for which it was obtained. This includes both internal and external parties – see paragraphs 43 and 44 below for more detail on sharing with consultants, contractors and partners. Refer any requests for access to personal data held by the SDS from third parties (i.e. external parties who are not given access in the normal course of business or under the terms of an existing partnership agreement) to the Corporate Office for advice. See paragraph 45 below for more detail on disclosure to the police and statutory agencies.

28. When disclosing personal data to third parties, take reasonable steps to confirm their identities. Be alert to the possibility of individuals attempting to obtain personal data by deception.

29. Ensure that further processing is compatible with the original purpose for which the data was obtained.

30. Seek the consent of the data subject for any new or non-obvious use or disclosure of the data.

31. Take reasonable steps to ensure that the data is accurate.

32. Take reasonable steps to ensure that data is kept up to date. This can often be done by contacting the data subject periodically and asking them to confirm continued accuracy or provide any updates.

33. Make sure that any inaccuracies discovered are promptly corrected, including situations where the data subject points out inaccuracies.

34. Ensure erasure or destruction of the data is in line with the SDS Retention Schedule.

35. Data subjects are entitled to access personal data on them that is processed by SDS. The SDS Data Protection Subject Access Procedure details how SDS must handle requests for personal data.

36. Ensure personal data is properly classified in line with the SDS Information Classification and Handling Policy.

37. Provide other employees and/or contractors with access to personal data only as required in relation to the purpose for which it was obtained.

38. Ensure personal data is stored in a secure manner, whether on computer or in hard copy.

39. Ensure opinions and expressions of intent are recorded in a way that would not cause embarrassment in the event of the data subject requesting access.

40. Remember that any reference to individuals in e-mails or correspondence is covered by the Act, and take appropriate care in relation to both content and who can see such communications.

41. Ensure data subjects have the opportunity to opt out of any proposed or potential direct marketing. This is an absolute right provided by the Act in most situations, but does not apply to SDS statutory services to young people.

## Compliance Requirements - Special Circumstances

42. There are additional steps which need to be taken in certain circumstances, as outlined below.

## Sharing Personal Data with Consultants, Contractors and Partners

43. In all cases where consultants or contractors are granted access to personal data, whether the processing of that data is the main purpose of the contract or incidental to it, the contract must include reference to the consultant's or contractor's obligations under the Data Protection Act, including their responsibility to maintain confidentiality. In addition, if the contractor is responsible for IS systems which process personal data on behalf of the SDS, consideration should be given to including specific reference in the contract to the need for adequate technical security over this data. Advice on contract terms can be obtained from the Procurement team and on security standards from EIS. Individual contractors engaged specifically for data processing roles involving the handling of personal data should be briefed on the implications of the Act.

44. Personal data may be shared with partner organisations where this is necessary in relation to the purpose for which the data was obtained, and in line with the relevant notification. Where a situation is identified where the sharing of personal data would be advantageous, but was not envisaged when the data was originally obtained, the consent of the data subjects should normally be obtained. Any new arrangements for sharing personal data with partners should be notified to the Data Protection Officer to ensure SDS's notification is updated.

## Disclosure of Personal Data to the Police and Statutory Agencies

45. SDS may receive requests for the disclosure of personal data from the Police, the Child Support Agency, Jobcentre Plus or other statutory agencies. In some cases we may be obliged to provide the information and in others disclosure is permissible if certain conditions are met. In general terms disclosure is likely to be legal if it relates to a specific investigation, but this is a complex area which may involve other legislation as well as the DPA and the legal advice should always be sought from the SDS Legal Team.

## Transfer of Personal Data Abroad

46. Data should not be transferred to any country or territory outside the European Economic Area[1] unless that country or territory has legislation which offers adequate protection for data, or at least one of certain other conditions is met. The ones most likely to apply are the consent of the data subject or that the transfer is necessary under a contractual obligation.

## Publishing

47. Images and recordings of identifiable individuals constitute personal data in terms of the Data Protection Act. Photographs, video and audio recordings of individuals should not be published in any material including promotional material or displayed on web sites, or in any other way made public without the consent of the individual concerned. In terms of the Act, publishing on the internet is regarded as worldwide transfer. Further advice can be obtained from the Data Protection Officer.

## Collection of Personal Data via the Internet

48. All SDS's websites must feature the corporate Privacy Statement. At any point where personal data is collected on-line there should be a link to this Privacy Statement.

49. The data collection screen should make mandatory only those fields which are necessary in relation to the purpose for which the data is being collected, and should make clear that completion of any other fields is optional. The screen, or a preceding screen, should make clear what will be done with the data, if this is not obvious. If it is intended to use the data for future marketing, an opt-out of such use must be provided. (Alternatively, an opt-in to such use may be offered). Further advice can be obtained from the Data Protection Officer.

## HR Records

50. SDS HR records include Recruitment and Selection, Employment Records, Equal Opportunities and Monitoring Records and Information on Employee's Health, e.g. occupational health records. Employees have the right to access their HR record. The SDS Data Protection Subject Access Procedure details how SDS must handle requests for personal data.

## Sensitive Personal Data

51. The Act defines a category of data called sensitive personal data. This consists of information about:

- Racial or ethnic origin;
- Political opinions;
- Religious or other similar beliefs;
- Trade Union membership;
- Physical or mental health;

[1] Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, UK.

- Sexual life;
- Offences (including alleged offences); and
- Criminal proceedings, outcomes and sentences.

52. Such information can only be processed if one or more of certain specified conditions are met. The full list is available in Appendix 1, paragraph 4. Within SDS it is anticipated that the ones most likely to apply are explicit consent of the data subject, legal employment obligation and equal opportunities monitoring.

53. In addition to ensuring that the pre-conditions are met, it is important to ensure appropriate security and confidentiality when processing sensitive personal data. In relation to equal opportunities monitoring, this involves limiting access to this data to the parties who undertake this monitoring. For example, in a recruitment situation monitoring data should be collected on a separate form which is not made available to the people making the selection of candidates for interview or carrying out the interviews.

## New Uses of Personal Data

54. Whenever a new IT system or business process which involves personal data is established, the Information Asset Owner should notify the Data Protection Officer to ensure that the DPA notification is updated accordingly.

55. Systems and process owners should also notify the Data Protection Officer if amendments are made to existing systems or processes involving the introduction of new classes of data subject or data, or new recipients of personal data.

# Appendix 1 - The UK Data Protection Act 1998

## 1. Scope

Data recorded on any type of electronic/magnetic form is within the scope of the Act.

This includes but not restricted too:

- PC/server hard drive;
- Floppy disk;
- CD Rom;
- DVD;
- Mobile phone/Blackberry memory;
- Personal organiser;
- Videotape;
- Memory stick; and
- Digital Storage.

Manual records created after 24th October 1998 are also included, if they are structured, i.e. filed alphabetically, numerically, etc. with reference to the data subject. Examples include:

- Address book;
- Telephone directory;
- Paper personnel files; and
- Photographs.

Since the Freedom of Information (Scotland) Act came into force (in January 2005), the rights of individuals to access data on themselves have been extended in the case of public bodies (including SDS) to information on any manual records.

## 2. The Eight Data Protection Principles

In the UK, if you hold or process data relating to a living individual, on any form of media (including paper from 24th October 2001), you are required to comply with the following principles of the Data Protection Act 1998.

These principles embody many of the main requirements of the European Directive 95/46/EC.

***Principle One*** - Personal data shall be processed fairly and lawfully.

***Principle Two*** - Personal Data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

***Principle Three*** - Personal Data shall be adequate, relevant and not excessive in relation, to the purpose or purposes for which they are processed.

***Principle Four*** - Personal Data shall be accurate and, where necessary, kept up to date.

***Principle Five*** - Personal Data processed for a purpose or purposes shall not be kept for any longer than is necessary for that purpose or purposes.

***Principle Six*** - Personal Data shall be processed in accordance with the rights of the data subject under the Act. These rights are:

- The right of access to personal data about him/her;
- The right to prevent processing likely to cause damage or distress;
- The right to prevent processing for the purposes of direct marketing; and
- Rights in connection with automated decision making.

***Principle Seven*** - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

***Principle Eight*** - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights of and freedoms of data subjects in relation to the processing of personal data.

## 3. Conditions for Processing Personal Data

The data subject has given his/her consent to the processing.

The processing is necessary for the performance of a contract to which the data subject is a party, or for taking steps to entering into a contract.

The processing is necessary for compliance with any legal obligation to which the data controller is subject.

The processing is necessary in order to protect the vital interests of the data subject.

The processing is necessary for the administration of justice, or for the exercise of any public function.

The processing is necessary for the purposes of legitimate interests of the data controller except where the processing prejudices the rights and freedoms or legitimate interests of the data subject.

## 4. Additional Conditions for Processing Sensitive Personal Data

The data subject has given his/her explicit consent to the processing of the personal data.

The processing is necessary for the purposes of any right or obligation under employment law.

The processing is necessary to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject.

The processing is necessary to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

The processing is carried out by any not for profit body for political, philosophical, religious or trade-union purposes, and relates only to its own members or associates and does not involve disclosure to a third party without consent.

The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

The processing is necessary for any legal proceedings, for the purpose of obtaining legal advice, or otherwise for the purposes of establishing, exercising or defending legal rights.

The processing is necessary for the administration of justice, or exercising any public function.

The processing is necessary for medical purposes and is undertaken by a health professional, or a person with equivalent duty of confidentiality.

The processing is of sensitive personal data on racial or ethnic origin, is necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and is carried out with appropriate safeguards for the rights and freedoms of data subjects.

## 5. Conditions for transferring Personal Data outside the EEA

The data subject has given his/her consent to the transfer.

The transfer is necessary under a contractual agreement between the data controller and the data subject.

The transfer is in the public interest.

The transfer is necessary for, or in connection with, legal proceedings, including the obtaining of legal advice, establishing/exercising/ defending of legal rights.

The transfer is in the vital interests of the data subject.

## 6. Subject Access Rights

Under the Act any individual is entitled to be told if any personal data is held about them and, if so:

- to be given a description of the data;
- to be told for what purposes the data are processed; and
- to be told the recipients or the classes of recipients to whom the data may have been disclosed.

They are also entitled:

- to be given a copy of the information with any unintelligible terms explained;
- to be given any information available to the controller about the source of the data; and
- to be given an explanation as to how any automated decisions taken about them have been made.

There are exemptions to some or all parts of the Act; however, these are mainly connected with law enforcement and national security. You should not assume exemptions apply to any of the data you are processing unless you have been authoritatively advised that this is the case.