SCDEA DATA PROTECTION
STANDARD OPERATING PROCEDURES

Version - V4.0, May 2010
Review Date - June 2011
Owner - Chair of Data, Records & Compliance Group

This document has been supplied for use with the Public Records (Scotland) Act 2011
Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01/03/2002</td>
<td>Karen Jackson-Morris, IAO</td>
<td>Changes to SPSA policy agreed at Data, Records &amp; Compliance meeting on 10/10/2007.</td>
</tr>
<tr>
<td>2.0</td>
<td>02/07/2009</td>
<td>Karen Jackson-Morris, IAO</td>
<td>Annual review by Data, Records &amp; Compliance Group. Updated p22 - “A supply of SAR forms is retained at SPSA offices and is available on the SPSA Public website.” Deleted footnote in para 6.2. To Governance Board for approval - change to para 4.5.1 - SCDEA Retention Schedule reference added.</td>
</tr>
<tr>
<td>3.0</td>
<td>13/12/2009</td>
<td>Karen Jackson-Morris, IAO</td>
<td>Added equality impact assessment to end.</td>
</tr>
<tr>
<td>4.0</td>
<td>14/05/2010</td>
<td>Karen Jackson-Morris, IAO</td>
<td>Annual review. Updated section 6 with new ICO power and monetary penalty.</td>
</tr>
</tbody>
</table>

Distribution

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Name(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01/03/2002</td>
<td>Policy Group</td>
</tr>
<tr>
<td>2.0</td>
<td>02/07/2009</td>
<td>SCDEA Intranet once approved by Governance Board</td>
</tr>
<tr>
<td>3.0</td>
<td>13/12/2009</td>
<td>SCDEA Intranet.</td>
</tr>
<tr>
<td>4.0</td>
<td>14/05/2010</td>
<td>SCDEA Intranet.</td>
</tr>
</tbody>
</table>

This document should not be disclosed, in whole or in part, to any third party without the prior express written consent of the Director General other than to SCDEA staff who have a 'need to know' and who have been made fully aware of these restrictions prior to disclosure; it should be used by SCDEA staff and permitted persons for the purpose for which it has been submitted and for no other.

No copying allowed, in any form, without prior written permission from the Director General, except as permitted under the Copyright, Design and Patents Act 1988.

Whilst every care has been taken in developing and compiling this document, the SCDEA accepts no liability for any loss or damage caused, arising directly or indirectly, in connection with reliance on its contents.
SCDEA DATA PROTECTION
STANDARD OPERATING PROCEDURES

1 Introduction ..................................................................................................................5

2 Intention .......................................................................................................................5

3 Definitions ...................................................................................................................5

4 The Data Protection Principles ....................................................................................5
   4.1 First Principle .........................................................................................................6
      4.1.1 Method of Compliance .................................................................................6
   4.2 Second Principle ....................................................................................................6
      4.2.1 Method of Compliance .................................................................................6
   4.3 Third Principle .......................................................................................................7
      4.3.1 Method of Compliance .................................................................................7
   4.4 Fourth Principle ....................................................................................................7
      4.4.1 Method of Compliance .................................................................................7
   4.5 Fifth Principle ......................................................................................................7
      4.5.1 Method of Compliance .................................................................................7
   4.6 Sixth Principle .......................................................................................................8
      4.6.1 Method of Compliance .................................................................................8
   4.7 Seventh Principle .................................................................................................8
      4.7.1 Method of Compliance .................................................................................8
   4.8 Eighth Principle ....................................................................................................8
      4.8.1 Method of Compliance .................................................................................8

5 Audit ...........................................................................................................................8

6 Offences Under the Act ...............................................................................................9
   6.1 Unlawful Obtaining or Disclosure .......................................................................9
   6.2 Enforced Subject Access .....................................................................................9

7 Responsibilities ........................................................................................................10

8 Appendix A - Definitions ..........................................................................................10
9 Appendix B – Conditions for Processing (Schedule 2 of the Act) ............ 14
10 Appendix C – Conditions for Processing (Schedule 3 of the Act) ............ 15
11 Appendix D – Subject Access Requests ........................................ 19
12 Appendix E – Subject Access Requests Flowchart and Guidance ............ 20
1 Introduction

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected.

Processing and transmission of personal data – generally information on living individuals who can be identified from the information – have legislative controls placed on them.

The Data Protection Act 1998 requires organisations to demonstrate to the Information Commissioner that they have adequate mechanisms in place to prevent against unauthorised or unlawful processing and accidental loss, damage or destruction of personal data.

The objective of this document is to provide management direction and support for data protection.

The policy will be subject to review annually and additionally in response to any changes affecting the basis of the original document. The policy will also be reviewed to monitor its effectiveness, demonstrated by the nature, number and impact of recorded incidents.

2 Intention

This policy sets out minimum standards for the collection and processing of personal data by the SCDEA and its business partners and contractors, where appropriate. It is intended to provide a common basis for developing organisational standards and effective management practice and to provide confidence in inter-organisational dealings and third party access/supply.

The policy extends to all personal data processed by SCDEA and in particular that which is processed on behalf of our business partners. Security requirements demonstrating compliance with Principle 7 of the Data Protection Act are contained in the separate SCDEA Information Security Policy and GPMS Policy.

3 Definitions

Definitions in relation to terminology are contained in Appendix A.

4 The Data Protection Principles

There are eight Data Protection Principles which data controllers are required to comply with. The principles apply to the processing of all personal data.

Separate procedures will be required for each data set/operating system where SCDEA is the data controller. These procedures must include detailed guidance in respect of compliance with each of the eight data protection principles.
4.1 First Principle

“Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

At least one of the conditions in Schedule 2 (Appendix B) is met; and in the case of sensitive personal data, at least one of the conditions in Schedule 3 (Appendix C) is also met.”

Meeting a Schedule 2 and Schedule 3 condition will not, on its own, guarantee that processing is fair and lawful. The general requirement that data be processed fairly and lawfully must be satisfied in addition to meeting the conditions.

4.1.1 Method of Compliance

SCDEA processes data in relation to its staff and also on behalf of its business partners. SCDEA is registered as a Data Controller in its own right, separate from the SPSA for specific “Purposes”. The SCDEA is solely responsible for compliance with the Act in terms of personnel data related to those “Purposes” and in addition has an obligation to ensure that, where personal data is processed on behalf of, or in conjunction with, a business partner, the processing is in accordance with this principle. SCDEA will provide a Notification to the Office of the Information Commissioner (OIC) in respect of the processing of personal data for specific “Purposes”. All other processing of personal data by SCDEA is processed under the SPSA’s Notification to the OIC, under the SPSA Data Protection Policy.

4.2 Second Principle

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be processed in any manner incompatible with that purpose or those purposes.”

There are two means by which a data controller may specify the purpose or purposes for which the personal data are obtained, namely:

(a) In a notice given by the data controller to the data subject in accordance with the fair processing requirements or,

(b) In a notification given to the Commissioner under the notification provisions of the Act.

4.2.1 Method of Compliance

SCDEA shall ensure, where practicable, that data subjects are advised of the purpose of the collection of their information. Where information has been obtained for a specific purpose, subject to the exemptions, any non-obvious use will be communicated to the data subject.

Where SCDEA receives a request for disclosure of information belonging to a business partner, the request shall be referred to the information owner, except where agreements are in place to facilitate disclosure via SPSA.
4.3 Third Principle

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.”

4.3.1 Method of Compliance

SCDEA will identify and collect the minimum amount of information that is necessary for the purpose. If it becomes necessary to hold/obtain additional information about certain individuals, such information will only be collected and recorded in relation to those individuals.

4.4 Fourth Principle

“Personal data shall be accurate and, where necessary, kept up to date.”

4.4.1 Method of Compliance

SCDEA shall instigate an audit programme to ensure that all relevant information, such as personnel records, are kept accurate and up to date.

Where appropriate an indicator with the last date of review shall be added to files.

Where SCDEA identifies an inaccuracy, or a data subject indicates that information held by SCDEA or supplied to a business partner is inaccurate, the error must be rectified by the owner of the data. Where SCDEA is not the owner, the owner must be advised without delay and in any case within forty-eight hours.

4.5 Fifth Principle

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that or those purpose."

4.5.1 Method of Compliance

SCDEA shall follow a documented procedure in relation to the retention of personal data in accordance with the SCDEA Retention Schedule. Personal data may not be retained on the basis that it might possibly be useful in the future.
4.6 Sixth Principle

“Personal data shall be processed in accordance with the rights of data subject in terms of the Data Protection Act 1998.”

4.6.1 Method of Compliance

Where SCDEA is notified as a Data Controller requests for subject access must be complied with within 40 days, subject to receipt of all necessary information. A maximum fee of ten pounds may be charged.

The subject access process is outlined in Appendix D.

4.7 Seventh Principle

“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.”

4.7.1 Method of Compliance

SCDEA has a separate Information Security Policy and GPMS Policy to address the requirements of this principle.

4.8 Eighth Principle

“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 of the rights and freedoms of data subjects in relation to the processing of personal data.”

4.8.1 Method of Compliance

In the event that SCDEA has a requirement/business need to transfer data out-with the EEA, guidance must be sought from the SPSA Information Assurance Officer based at the SCDEA.

5 Audit

In order to ensure the continued compliance with the Data Protection principles, SCDEA will develop an audit plan based on a risk assessment and will audit the data in accordance with best practice.

The overriding objective of auditing is to ensure that data held in computer systems is obtained, held, used and disclosed in accordance with the Data Protection Act and other relevant legislation.
The results of audits shall be communicated to the relevant SCDEA Management meetings.

6 Offences Under the Act

6.1 Unlawful Obtaining or Disclosure

It is an offence for a person, knowingly or recklessly, without the consent of the data controller, to:

- Obtain or disclose personal data or the information contained in personal data, or
- Procure the disclosure to another person of the information contained in personal data.

The Information Commissioner Office's (ICO) new power (under sections 55A and B of the DPA) to issue monetary penalties came into force on 6 April 2010, allowing the ICO to serve notices requiring organisations to pay up to £500,000 for serious breaches of the DPA. The ICO has produced statutory guidance about how it proposes to exercise this new power, which has been approved by the Secretary of State for Justice, available at: [http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf)

In brief, the Commissioner may impose a monetary penalty notice if a data controller has seriously contravened the data protection principles and the contravention was of a kind likely to cause substantial damage or substantial distress. In addition the contravention must either have been deliberate or the data controller must have known or ought to have known that there was a risk that a contravention would occur and failed to take reasonable steps to prevent it.

6.2 Enforced Subject Access

Unless one of the statutory exceptions apply it is an offence for a person to require another person or a third party:

- to supply him with a relevant record; or
- to produce a relevant record to him;

in connection with:

- The recruitment of that person as an employee;
- The continued employment of that other person;
- Any contract for the provision of services to him by that other person; or
- Where a person is concerned with providing (for payment or not) goods, facilities or services to the public or to a section of the public, as a condition of providing or offering to provide any goods, facilities or services to that other person.
7 Responsibilities

Heads of Business Areas are responsible for ensuring compliance with the Data Protection Act in their business area.

The SPSA Information Assurance Officer based at the SCDEA is responsible for ensuring that a valid notification is maintained with the Office of the Information Commissioner in respect of SCDEA’s processing.

The SPSA Compliance Manager is responsible for ensuring that a valid notification is maintained with the Office of the Information Commissioner in respect of SPSA’s processing.

All staff will receive appropriate training/briefings in accordance with the information handled within their job role.

8 Appendix A - Definitions

Data (Including manual data/relevant filing system)

Data means information which:
- Is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- Is recorded with the intention that it should be processed by the means of such equipment;
- Is recorded as part (or with the intention that it should form part) of a relevant filing system (i.e. any set of information relating to individuals to the extent that, although not processed as in (a) above, the set is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible); or
- Does not fall within (a), (b) or (c) but forms part of an ‘accessible record’. An accessible record is defined in Section 68 of the Act.

Personal Data

Personal data is defined in the Act as ‘data which relate to a living individual who can be identified:

- From those data; or
- From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller’

This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Therefore, according to the definition of the Act, where an individual is capable of being identified from data which relate to that individual, such data are personal data.
Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including:
Organisation, adaptation or alteration of the information or data;
Retrieval, consultation or use of the information or data which, in relation to personal data, includes using the information contained in the data;
Disclosure of the information or data which, in relation to personal data, includes disclosing the information contained in the data by transmission, dissemination or otherwise making available, or
Alignment, combination, blocking, erasure or destruction of the information or data

Data Subject
Data subject means ‘an individual who is the subject of personal data’. A data subject must be a living individual. A data subject need not be a UK national or resident.

Data Controller
A Data Controller is defined as “A person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed”.
A data controller must be a “person”, i.e. a legal person. This term comprises not only individuals but also organisations such as companies and other corporate and unincorporated bodies of person.
A data controller must decide the purpose for which personal data are, or will be, processed and the way in which the data are, or will be, processed.

Data Processor
In the context of the Act, Data Processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
The data controller retains full responsibility for the actions of the data processor.

Third Party
‘Third party, in relation to personal data, means any person other than:
The data subject
The data controller, or
Any data processor or other person authorised to process data for the data controller or processor’.
The expression third party does not include employees or agents of the data controller or data processor.
Sensitive Personal Data

The Act defines categories of sensitive personal data, namely personal data consisting of information as to:

- The racial or ethnic origin of the data subject;
- His/her political opinions;
- His/her religious beliefs or other beliefs of a similar nature;
- Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- His/her physical or mental health or condition;
- His/her sexual life;
- The commission or alleged commission by him/her of any offence; or
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.
Appendix B – Conditions for Processing (Schedule 2 of the Act)

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):

- The data subject has given his consent to the processing (see paragraph 3.1.5 below).
- The processing is necessary –
  (a) for the performance of a contract to which the data subject is a party; or
  (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The processing is necessary in order to protect the vital interests of the data subject.

The Commissioner considers that reliance on this condition may only be claimed where the processing is necessary for matters of life and death, for example, the disclosure of a data subject’s medical history to a hospital casualty department treating the data subject after a serious road accident.

- The processing is necessary –
  (a) for the administration of justice;
  (b) for the exercise of any functions conferred by or under any enactment;
  (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department;
  (d) for the exercise of any other functions of a public nature exercised in the public interest.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.
10 Appendix C – Conditions for Processing (Schedule 3 of the Act)

At least one of the following conditions must be satisfied, in addition to at least one of the conditions for processing in Schedule 2 (which apply to the processing of all personal data), before processing of sensitive personal data can comply with the First Principle:

- The data subject has given his explicit consent to the processing of the personal data;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

The Secretary of State may specify cases by order where this condition is either excluded altogether or only satisfied upon the compliance with further conditions. No order has been made to date to this effect.

- The processing is necessary –
  (a) in order to protect the vital interests of the data subject or another person, in a case where –
     (i) consent cannot be given by or on behalf of the data subject, or
     (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
  (b) in order 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 –
  (a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade union purposes and which is not established or conducted for profit;
  (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
  (c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes; and
  (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

Each of these provisions needs to be satisfied in order to fall within this condition. However, the Commissioner is of the view that data controllers who rely upon this condition as a basis for processing may make subsequent non-consensual disclosures of sensitive personal data only if there is a basis for doing so under one of the other Schedule 3 conditions. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
The processing –
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

The Commissioner’s view is that (c) above is of limited scope and data controllers should adopt a narrow interpretation and rely upon another Schedule 3 condition if there is any doubt as to whether it applies. In particular, it should not be used to construct a legal right where none exists.

The processing is necessary –
(a) for the administration of justice;
(b) for the exercise of any functions conferred by or under any enactment; or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied if further specified conditions are met.

The processing is necessary for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by –
(a) a health professional (as defined in section 69 of the Act); or
(b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

The processing
(a) is of sensitive personal data consisting of information as to racial or ethnic origin;
(b) is necessary for the purpose of 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
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects. The Secretary of State may specify by order circumstances in which such processing is, or is not, to be taken as carried out with appropriate safeguards for the rights and freedoms of data subjects. No order to this effect has been made to date.

The personal data are processed in circumstances specified by order made by the Secretary of State. Currently the only such order is the Sensitive Data Order. This includes detailed provisions for:

(1) processing that is in the substantial public interest and is necessary for the prevention or detection of any unlawful act and must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes; or
(2) processing that is in the substantial public interest and is necessary for the discharge of any function which is designed for protecting members of the public against:

- dishonesty, malpractice, or other seriously improper conduct by, or the unfitness of incompetence of, any person, or
- mismanagement in the administration of, or failure in services provided by, any body or association, and
- must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the discharge of that function; or

(3) the disclosure of personal data that is:

(i) in the public interest and
(ii) is in connection with:

the commission by any person of any unlawful act (whether alleged or established), or dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established), or mismanagement in the administration of, or failures in the services provided by, any body or association (whether alleged or established)

(iii) is for the special purposes as defined in section 3 of the Act; and (iv) is made with a view to the publication of those data by any person and the data controller reasonably believes that such publication would be in the public interest.

(4) processing that is:

(i) in the substantial public interest;
(ii) is necessary for the discharge of any function which is designed for the provision of confidential counseling, advice, support or any other service; and
(iii) is carried out without the explicit consent of the data subject because the processing:

- is necessary in a case where consent cannot be given by the data subject, or
- is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent, or
- must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, support, advice or other service.

(5) processing that:

(i) is necessary for the purpose of:
• carrying on an insurance business (as defined); or
• making determinations in connection with eligibility for, and benefits payable under, an occupational pension scheme (as defined),
(ii) is of sensitive personal data relating to the physical or mental health or condition of the data subject who is the parent, grandparent, great grandparent or sibling of the insured person or member of the scheme;
(iii) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject and the data controller is not aware of the data subject withholding his consent; and
(iv) does not support measures or decisions with respect to the data subject.

(6) processing of sensitive personal data in relation to any particular data subject that are subject to processing already under way immediately before 1 March 2000 and where the processing is necessary for carrying on insurance business or establishing or administering an occupational pension scheme, where such processing is either;

(i) necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject and the data subject has not informed the data controller that he does not so consent; or
(ii) it must necessarily be carried out even without the data subject’s explicit consent so as not to prejudice those purposes.
For an explanation of “processing already under way” and transitional relief, see Chapter 6.

(7) processing of sensitive personal data consisting of information as to religious beliefs (or other beliefs of similar nature) or physical or mental health or condition where:

(i) the processing is necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons with a view to enabling such equality to be promoted or maintained; and
(ii) it does not support measures or decisions relating to a data subject otherwise than with the data subject’s explicit consent; and
(iii) it does not cause nor is likely to cause substantial damage or distress to the data subject or any other person.

The data subject has the right to prevent such processing by notice in writing to the data controller.

(8) processing of personal data consisting of information as to the data subject’s political opinions that is carried out by certain people or political organisations where it does not cause nor is likely to cause substantial damage or substantial distress to the data subject or any other person.
Again, the data subject has the right to prevent such processing by notice to the data controller.

(9) processing that
(i) is in the substantial public interest;
(ii) is necessary for research purposes (as defined in section 33 of the Act);
(iii) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject;
(iv) does not cause nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

(10) processing that is necessary for the exercise of any functions conferred on a constable by any rule of law.

11 Appendix D – Subject Access Requests

SCDEA has a duty under the DPA 1998 to respond to subject access requests where the Director General is a data controller.

Where processing is being undertaken the data subject will be given a description in writing of:

- The personal data
- The purpose for which they are being processed; and
- To whom they are or may be disclosed

Where the information belongs to or has been obtained from a third party, the third party will be contacted prior to any disclosure of personal data.

The information given in response to a subject access request will, subject to exemptions, be all that which is contained in the personal data at the time the request was received. However, routine planned amendments and deletions of the data may continue between the date of the request and the date of the reply. Having received a request, SCDEA will not make any special amendment or deletion which would not otherwise have been made.

Where SCDEA becomes aware of an inaccuracy in the data stored through receipt of a subject access request, the original data, including any errors, must be supplied to the data subject. However, SCDEA will correct the information and provide the data subject with a copy of the amended data.

Where an application for information is made through a third party, a mandate, signed by the data subject will be required. In order to protect the interests of the data subject and prevent unauthorised disclosures it is anticipated that such requests will only be received from Solicitors, or Legal Representatives (guardians, power of attorney).
12 Appendix E – Subject Access Requests Flowchart and Guidance

Subject Access Requests
Data Protection Act (1998)
Flowchart Guidance

Subject Access Request (SAR) received

The SCDEA will use the SPSA SAR form. A supply of SAR forms is retained at SPSA offices and on the SPSA Public website. Forms may be obtained by contacting the Compliance Section, Elphinstone House, 65 West Regent Street, Glasgow, G2 2AF.

The request must be in writing and must include the prescribed fee (£10) and a suitable form of identification, such as photocopy of driving licence, passport, birth certificate, utility bill (last three months). Where the subject presents in person to make a request original identification documents may be checked by the person accepting the request. The details of the identification seen must then be logged in the appropriate section of the subject access form.

SCDEA must respond to requests within 40 calendar days and as such all requests for information must be notified/forwarded to the Compliance Section within 3 working days.

Who is the requestor?

Generally the request should be made by the data subject themselves. Exceptions are children under 12\(^2\) and legal representatives. Where the request is from a parent/guardian a copy of the childs birth certificate will be required. Where the request is from a legal representative a mandate, signed by the data subject and accompanied by identification, will be required.

Requests must not be accepted from third parties, such as employers and responses will only be sent back to the requestors home address or their legal representative.

Requests for personal data from third parties in respect of legal proceedings/prospective legal proceedings must be forwarded to the SPSA Compliance Section within 3 working days.

Third Party Data

Where the information requested contains 3\(^{rd}\) party data (another persons name etc) that data must either be redacted or consent obtained from the 3\(^{rd}\) party for disclosure.

Where the information requested contains data provided by another organisation, that organisation must be contacted prior to disclosure.

---

\(^2\) A child of 12 or over will generally be deemed to have the capacity to make a request
Diversity

There is no adverse impact on any group in terms of race, religion, gender, sexuality, disability or age in relation to this procedure. The application of this policy/procedure will be monitored to ensure compliance with the organisation’s Equality and Diversity Strategy.

Health & Safety

There are no specific additional issues in relation to health and safety relating to this procedure.

Communication

This policy/procedure is available to all SCDEA staff via the Intranet. The SCDEA Governance Board is responsible for ensuring that staff are made aware of the policy/procedure and their responsibilities arising from its operation.

Monitoring and Review

This policy/procedure will be reviewed annually by the document owner.