

Data Protection Code of Practice Archive Collections

March 2016

CONTENTS

1. INTRODUCTION	3
2. PRESERVATION OF PERSONAL DATA AS ARCHIVES	3
3. APPRAISAL	4
4. ACCESSIONING	5
5. FREEDOM OF INFORMATION	8
6. RESPONSIBILITIES FOR DATA PROTECTION	8
7. RESTRICTIONS ON ACCESS	10
8. RECORDS RECLOSURE	13
9. FINDING AIDS	15
10. SECURITY OF ARCHIVES	17
11. ACCESS TO PERSONAL DATA IN ARCHIVES	17
ANNEX A: DEFINITION OF SUBSTANTIAL DAMAGE AND DISTRESS	22
ANNEX B: DEPOSITOR QUESTIONNAIRE	23

1. Introduction

- 1.1 National Records of Scotland (NRS) is required by law to comply with the Data Protection Act 1998 (the Act), which was enacted to ensure the fair and lawful processing of personal data. This code of practice has been drawn up to ensure NRS complies with the legislation by following corporate wide policies and procedures for the management and administration of archive collections transferred to NRS for permanent preservation. It does not apply to information created or received by us in the course of our business transactions, which is subject to a separate code¹.
- 1.2 NRS regards the lawful and correct treatment of personal information as integral to successful business operations and to maintaining the confidence of our customers and stakeholders. Our commitment to effective data protection is supported by the *NRS Data Protection Policy*. This requires every member of staff to familiarise themselves with and follow NRS data protection policy, guidance and practices, of which this code forms a part.
- 1.3 The National Archives, the Archives and Records Association (formerly the Society of Archivists), the Information and Records Management Society and the National Association for Information Management have produced a *Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998 (2007)*. This document provides wider guidance on data protection issues as they relate to archivists and records managers and colleagues are advised to consult this as appropriate.
- 1.4 This code of practice applies only to records of living individuals covered by the Act. In Scotland the lifetime of an individual is generally considered to be 75 years for an adult and 100 years for a child and restrictions on access to records containing the personal data of living individuals are commonly applied on this basis. However, within the rest of United Kingdom the lifespan of an individual is assumed to be 100 years and some of our record depositors have chosen to apply access restrictions accordingly.

2. Preservation of Personal Data as Archives

- 2.1 The Act defines personal data as data which relate to a living individual who can be identified:
 - (a) from those data, or;

¹ Please see the *Data Protection Code of Practice: Business Information*.

- (b) 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.

2.2 The Act requires organisations and individuals who handle personal information to comply with eight data protection principles². Principle 2 of the Act states that personal data shall only be collected for one or more specified and lawful purposes and further processing shall be compatible with those purposes. Principle 5 states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

2.3 The Information Commissioner has approved the following special purpose as a compatible further use of personal data:

*Records selected for permanent preservation as archives, with a view to their use in historical or other research.*³

2.4 Personal data may be retained as archives for research purposes indefinitely provided that:

- the data are not processed to support measures or decisions with respect to particular individuals, and;
- the data are not processed in such a way that substantial damage or distress is, or is likely to be, caused to any data subject.⁴

2.5 Some archives which NRS processes for the purposes of archival preservation may also for a period retain a business use for the depositing bodies and therefore can also be preserved for these purposes.⁵

3. Appraisal

3.1 Personal data which merits permanent preservation should be identified and scheduled for retention as soon as possible. An over-rigorous interpretation of the Act may result in record creators taking unnecessary action to weed, redact or

² Please refer to the *Data Protection Policy* for details of these principles.

³ Processing for the purposes of archival preservation can be undertaken with regard to the exemptions set out in section 33 of the Act: research, history and statistics.

⁴ For the meaning of 'substantial damage and distress' see Annex A.

⁵ NRS regularly retransmits to the Crown Office, Scottish Court Service and the Scottish Government Department and Agencies archives which the depositors wish to use for current business purposes. Access to archives may also be requested by individuals or organisations other than the depositor for current business uses e.g. the Scottish Criminal Cases Review Commission may request access to court records when reviewing individual cases.

destroy records containing personal data that would otherwise be archived. Stakeholders and other potential depositors should be made aware that NRS can store personal and sensitive personal data for research purposes.

- 3.2 When deciding whether to permanently preserve records containing sensitive personal data you must consider whether their value for research purposes justifies their retention and is in the substantial public interest.
- 3.3 Appraisal should be carried out within the framework of the accessioning branch's selection policy⁶ and appraisal decisions should be documented on the relevant collection policy file.

4. Accessioning

- 4.1 All archives accessioned by NRS should be surveyed to determine whether they include personal data covered by the Act. Prior to their physical transfer, NRS should seek answers from the donor or depositor to the following questions⁷, a record of which should be kept on the appropriate collection policy file:

- *Do the archives contain personal data already covered by a notification to the Information Commissioner? If so, obtain details of the notification.*
- *Are any personal data exempt from subject access?⁸*
- *Does the deposit include any sensitive personal data as defined by the Act? If so specify the category of sensitive personal data.*
- *What data protection role will NRS assume for the archives? This issue should be discussed and agreed between NRS and the depositor.*

⁶ Policy on the Selection of Government Records; Policy on the Acquisition and Retransmission of Private Records; Draft Policy on the Selection of Court and Legal Records.

⁷ For a depositor questionnaire, see Annex B.

⁸ Data is exempt from subject access if it is already available in the public domain - for example public registers.

4.2 Recording Accessions on CALM:

When NRS acquires personal data for archival preservation it must demonstrate, in accordance with Principle 1, that there is a fair and lawful basis for doing so. Processing must be justified by a relevant condition under Schedule 2 of the Act: PERSONAL DATA		
Criteria Reference	Record Type	Justification
A1	Public Records	<p>The data are retained because the processing is necessary:</p> <p><i>a) for the exercise of any functions conferred on any person by or under any enactment [e.g. The Public Records (Scotland) Act 1937 or The Public Registers and Records (Scotland) Act, 1948] (Schedule 2 5(b))</i></p> <p><i>b) for compliance with any legal obligation to which the data controller is subject (Schedule 2 (3)), or</i></p> <p><i>c) for exercise of any other functions of a public nature exercised in the public interest by any person (Schedule 2 5(d))</i></p>
A2	Private Records	<p>The data are retained because the processing is necessary:</p> <p><i>a) for exercise of any other functions of a public nature exercised in the public interest by any person (Schedule 2 5(d)) This is applicable to some private sector bodies which have a public interface, such as charities, churches or academic bodies. This is also applicable to NRS as it makes records available to the public; or</i></p> <p><i>b) for the purposes of legitimate interests pursued by the data controller [depositor] or by the third party or parties to whom the data are disclosed [NRS and researchers], except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. (Schedule 2 6(1)) Archives of companies or private families may be acquired for historical preservation where there is a legitimate business interest or family interest to preserve this information.</i></p>

The processing of sensitive data must be further justified by a relevant condition under Schedule 3 of the Act or SI 2000 No. 417, The Data Protection (Processing of Sensitive Personal Data) Order 2000:

SENSITIVE PERSONAL DATA		
Criteria Reference	Record Type	Justification
B1	Public Records	The data are retained because the processing is necessary: <i>a) for the exercise of any functions conferred on any person by or under any enactment (Schedule 3 7(1)(b)), or b) for the exercise of any functions of the Crown, a Minister of the Crown or a government department (Schedule 3 7(1)(c))</i>
B2	Public and Private Records	The data are retained because the processing is: <i>a) is in the substantial public interest; b) is necessary for research purposes (which expression shall have the same meaning as in section 33 of the Act); c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject; and d) does not cause, nor is likely to cause, substantial damage or distress to the data subject or any other person. SI 2000 No. 417, The Data Protection (Processing of Sensitive Personal Data) Order 2000 (9)</i>

- 4.3 When acquiring records for deposit you should note on the accession record the criteria under which NRS is fairly and lawfully acquiring the personal data. In the Access Conditions field you should note:

This accession contains personal/sensitive personal data covered by the Data Protection Act 1998. Its accession is fair and lawful and fulfils criteria reference(s) [insert reference(s)] as outlined in the NRS Data Protection Code of Practice on Archival Information.

It is also useful to record the location of personal and sensitive personal data in an accession, for example noting 'personal data in box 8 only'.

5. Freedom of Information

- 5.1 All archives created or owned by bodies subject to the Freedom of Information (Scotland) Act (FOISA) or the Freedom of Information Act (FOIA) and containing personal data of identifiable living individuals are subject to the Act. An exemption can be applied under section 38 of FOISA or section 46 of FOIA, as relevant, if either confirmation of the existence of the data or its release would breach any of the Data Protection Principles. Depositors who are subject to FOI should prepare a schedule identifying exempt information before they transfer records to NRS for permanent preservation.
- 5.2 It is generally the responsibility of the transferring authority to identify this information. However, it may not always be practical for the depositor to prepare an individual schedule of all the records they have created. In such instances a restriction on access can be applied on a series wide basis. If a researcher requests access to a record from a restricted series the depositor will review the record at this point and any information that can be made available under FOI will be released and the catalogue updated to reflect this.
- 5.3 As NRS is a public body, personal data of private origin will fall under FOISA if ownership has passed to NRS. Private records held on deposit are not subject to FOISA.

6. Responsibilities for Data Protection

- 6.1 The data protection roles of NRS and the depositor of archives should be agreed when the records are accessioned and recorded in a deposit agreement. NRS should take on one of the following data protection roles:
- 6.2 **Role of Data Processor** - NRS acts as data processor of the archives in its custody, processing data on behalf of the depositor who remains data controller. As data processor NRS will not be responsible for any data processing decisions, including whether to provide subject access. Subject access requests specifically for data contained in collections covered by this type of deposit arrangement must be handled by the data controller. If NRS receives a subject access request they will instruct the person making the request to resubmit their request directly to the data controller.

The following statement should be included in the deposit agreement:

[The client] retains the status of data controller as defined in section 1(1) of the DPA 1998 for any personal data transferred to the Keeper of the Records of Scotland. [The client] appoints the Keeper to act exclusively as a data

processor as defined under section 1(1) of the DPA 1998. Should the Keeper receive a data subject access request for information which may be held in transferred records and which are not yet publicly available, he will inform the person making the request that they must make their request directly to [the client]. The Keeper's staff will assist [the client] as far as possible to ascertain whether information about the data subject is held and where appropriate retransmit the records to [the client] or make arrangements for access to the records at NRS.

- 6.2 **Role of Data Controller** - NRS assumes sole responsibility for all data protection issues, determining the purposes for which personal data may be processed.

The following statement should be included in the deposit agreement:

[The client] gives this material, and any additions which [the client] makes to it, unencumbered to the Keeper of the Records of Scotland and appoints the Keeper to act as the sole data controller, to determine the purposes for which and the manner in which any personal data are, or are to be, processed.

- 6.3 **Role of Joint Data Controller** - NRS acts as joint data controller along with the depositor. This shared role allows depositors to remain involved in decisions affecting the administration of the personal data contained within their records. Any data protection issues, such as decisions made about access restrictions, will be determined by both parties. NRS will be able to respond to subject access requests relating to data in the deposited records. If this option is agreed NRS should provide the depositor with a note of the responsibilities the Keeper agrees to undertake under the role of joint data controller.

The following statement should be included in the deposit agreement:

[The client] gives custody of this material, and any additions which [the client] makes to it, to the Keeper of the Records of Scotland and appoints the Keeper to act as a joint data controller, to determine, in collaboration with [the client] the purposes for which and the manner in which any personal data are, or are to be, processed.

- 6.4 **Defunct Bodies** - Where NRS holds records of a defunct body, an appropriate arrangement should be negotiated with its successor organisation if one exists. If there is no obvious successor to the original record creator then the responsibilities of data controller will be assumed de facto by the Keeper. Such cases should be infrequent.

The following statement should be included on the collection policy file:

This collection was passed to the Keeper of the Records of Scotland's authority. The creating body no longer exists and no successor body exists to act as data controller to the collection. Therefore, the Keeper assumes the responsibilities of the sole data controller, to determine the purposes for which and the manner in which any personal data are, or are to be, processed.

- 6.5 ***Gifts, Legacies and Purchases*** - NRS will be sole data controller for archives which it has been gifted or bequeathed or has purchased.
- 6.6 ***Deposits*** - NRS can act as data controller, joint data controller or data processor for archives which have been deposited in custody of NRS, but ownership retained by the depositor.
- 6.7 ***Government Records*** - Records of the Scottish Government are subject to a service level agreement, which defines data protection roles and responsibilities.⁹
- 6.8 ***Court and Legal Records*** - Records are transmitted from the Supreme Courts, sheriff courts and various other bodies exercising functions derived from the courts (e.g. Accountant in Bankruptcy) under the Public Records (Scotland) Acts 1937 and 2011. Records of the High Court of Justiciary are transmitted according to an Act of Adjournal, records of the Court of Session according to an Act of Sederunt, and records of the sheriff courts by agreement of Sheriff Principal. Records created by the Registers of Scotland are transmitted under the Public Registers and Records (Scotland) Act 1948. Agreements have been established with each of the depositors which outline data protection roles and responsibilities.

7. Restrictions on Access

7.1 Determining Restricted Access Periods

Archival material which contains personal and sensitive personal data may be subject to periods of closure or restricted access. NRS will determine the appropriate periods of records for which it is sole data controller. Where NRS is the joint data controller or data processor periods should be determined in consultation with the depositors of the records. Any decisions taken on restricting access should be documented and recorded onto the collection policy file and noted in the catalogue.

⁹ 'Service Level Agreement between National Records of Scotland, Government Records Branch and Scottish Government, Human Resources & Corporate Services, Information Services & Information System, Information Management Unit' (November 2009).

7.2 Personal Data

Archives containing personal data should be considered on a case by case basis to determine the appropriate period of restricted access. It is not practical to provide rigid guidelines as the length of closure will depend on the type of personal information and its context. Where the archives contain large quantities of personal data, as with court records, a series wide restriction may be applied.

7.3 Sensitive Personal Data¹⁰

Access to archives containing sensitive personal data, the disclosure of which could cause substantial damage or distress to the data subject, should be restricted for the lifetime of the individual. In Scotland this is generally considered to be 75 years for an adult or 100 years for a child. However, some record depositors may decide to assume a lifespan of 100 years for an adult in line with opinion within the rest of United Kingdom.

7.4 Deceased Health Records

Please also note that although the Act concerns the data of living individuals, it is worth stressing that health records of a deceased person are exempt under section 38 of FOISA for a period of 100 years after the date of the last entry in the records.¹¹

7.5 Other Personal Data

Some types of personal data may be disclosed sooner for the purpose of historical research if access is considered fair and lawful. When considering whether archives containing personal data can be made available for research access the following criteria should be considered:

- *Statutory Requirements* - Statutes protecting the confidentiality of personal information must be respected. For example, the Adoption and Children (Scotland) Act 2007 or the Criminal Procedure (Scotland) Act 1995.
- *Information must not be Defamatory or Obscene* - Information relating to a named individual must not include false statements about the person that may injure the reputation of that person to the extent that it would be likely to cause them substantial damage or distress. Nor should information be offensive to the extent that it would cause the named person substantial damage or distress.

¹⁰ Please see the *Data Protection Policy* for a definition of sensitive personal data.

¹¹ Health records encompass not just medical records, but also other records such as psychological reports contained among court papers.

- *Public Domain* - Genuine information (as opposed to speculation) already in the public domain because it as a matter of public record should be accessible.
- *Age* - Sensitivity erodes over time. The age and status of the data subject should be considered, where this can be ascertained. Where possible, the age and status at the time the record was created and the age and status at the time of cataloguing should also be considered.¹²
- *Nature* - Some personal data, including sensitive data, can be relatively innocuous and as such its disclosure is unlikely to cause substantial damage or distress. For example, the disclosure of information about admission to hospital 20 years ago for a broken bone is unlikely to cause concern, whereas it would be reasonable to assume that an individual would not want information about the treatment of mental illness disclosed.
- *Record Creator* - The views of the record creator(s), if they have retained the role of data controller, should be consulted when deciding on the suitability of closure periods.
- *Records subject to FOI* - Personal data in archives subject to FOISA are exempt under section 38 of FOISA if either confirmation of the existence of the data or its release would breach any of the Data Protection Principles. Similarly personal data in archives subject to FOIA are exempt under section 46 of the FOIA. An exemption should be applied to these records and noted in the catalogue. 'Exempt' should be entered in the Access Status field and the following wording entered in the Access Conditions field:

Some information in this item is exempt under Section 38 of the Freedom of Information (Scotland) Act 2002: Personal Information and as such will not be available for public consultation until [closed until date]. To request access to it whilst the exemption is current, please contact the Corporate Planning & Development Team.

Although the Act concerns the data of living individuals, it is worth stressing that health records of a deceased person are also exempt under section 38 of FOISA for a period of 100 years after the date of the last entry in the records.

- *Records not subject to FOI* - For archives containing personal data which are not subject to FOI an appropriate period of restricted access should be applied. 'Restricted' should be entered in Access Status field of the catalogue

¹² This may not always be practical, as, for example, with court records where neither NRS nor the depositing courts possess the resources to examine individually the hundreds of case transferred annually to NRS.

and 'Access restricted to [insert reference] records for [insert number] years for Data Protection requirements' in the Access Conditions field.

8. Records Reclosure

8.1 It is uncommon for a record which is open to be subsequently withdrawn from public access, but there are legitimate circumstances when this may be required. The NRS Records Reclosure Policy explains why this may happen and how a decision on reclosure may be reached.

8.2 Reasons for Reclosure

The reasons why an open record may need to be closed will vary, but the following are likely to be the most common reasons: .

- A record may be found to contain personal or sensitive personal information about a living individual and disclosure of this information to the public would be unlawful or unfair under the Data Protection Act 1998, or would breach the individual's right, or that of their family, to a private and family life under the Human Rights Act 1998.
- A record may have previously been opened in good faith, but the circumstances in which it was opened have changed and a reclosure is now considered appropriate.
- A record may have been opened in error and its reclosure is necessary to correct this mistake.

8.3 Reclosure Process

Records will be considered for reclosure on receipt of external requests from a record depositor or a member of the public, or following a referral by a member of NRS staff. Requests should be submitted in writing to the NRS Data Protection and Freedom of Information Officer.

When a request is received the record will be temporarily closed to the public while an assessment takes place and the catalogue will be updated to reflect that this is happening. If a digital image of the record has been published on our websites or on the internal online resources in our search rooms then the image will also be temporarily taken down.

The assessment will be carried out by an NRS panel which includes the NRS Data Protection and Freedom of Information Officer and relevant specialists. The panel will be chaired by the Information Asset Owner of the records being assessed.

The panel will consider the issues and reach a recommendation on whether a record should be closed or remain open, but the final decision on access will be taken by the data controller of the record. The Keeper is data controller of some of the records in his custody, but in many cases this role has been retained by the public authority, organisation, family or individual who deposited the records with NRS. The Registrar General is data controller of the statutory registers.

If the panel and data controller determine that a record should be closed its access status will be amended in line with the restrictions placed on other closed records. If the panel and data controller decide that the record should not be closed, its access status will revert to open. However, should a data controller decide that a record should be open against the recommendation of the panel, NRS will not facilitate what it considers to be inappropriate access.

If only some of the information needs to be withheld then the remainder of the record will be opened again to public access or a surrogate copy with appropriate redactions made available. If a record is closed in full or in part the date at which it can be reopened will be published in the catalogue.

The assessment will be completed within 30 working days of the request being received.

8.4 **Decision Making**

To reach a recommendation on reclosure the Panel will take into account a range of considerations. These can include the age of the record, the length of time it has been in the public domain, whether the information is likely to be otherwise obtainable elsewhere, the opinion of the depositor / data controller, and, where applicable, the public interest in withholding the record from public access.

For public records the Panel will use the exemptions in the Freedom of Information (Scotland) Act 2002, Freedom of Information Act 2000 or the Environmental Information (Scotland) Regulations 2004 as an objective test.

8.5 **Takedown**

Where a digital image of a reclosed record has been previously published on any of our online resources, that image will also be taken down until such time as the record is reopened.

8.6 Appeals

If a member of the public who has requested the reclosure of a record disagrees with a decision not to carry this out they have the right to complain to the Chief Executive of National Records of Scotland. Appeals should be made by following our [complaints procedure](#), details of which are available on our website. Appeals must be submitted within 40 working days of being notified of the decision.

9. Finding Aids

- 9.1 Finding aids made available to the public, either in search rooms or over the Internet, are covered by the Act if they include entries containing personal information about living identifiable individuals. The inclusion of personal information in finding aids and indexes should in general terms be avoided, unless there is a specific value or need – for example to describe a personal case file or court case. When preparing finding aids a number of points should be borne in mind:
- 9.2 *Is the material open or closed?* - If the records themselves are closed, consider whether the information in the catalogue description in effect discloses the information that has caused the item to be closed.¹³ If it does, then consider removing the personal data from the description. If the information is open, then the description, if it is fair, accurate and unlikely to cause substantial distress or damage, should also be open and available to the public.
- 9.3 *Is the person alive or dead?* - If the person is known to be deceased their personal data can be included in the description. If the records described are over 75 years old (100 years for minors), then it may generally be assumed that neither they nor their description are subject to the provisions of data protection. For some records the depositor will have requested that an adult lifespan of 100 years be assumed and this should be taken into account accordingly. Please note that health records of a deceased person are exempt under section 38 of FOISA for a period of 100 years after the date of the last entry in the records.
- 9.4 *Is the person identifiable?* - Putting a name in a catalogue does not really fully identify the person. However if the description provides a name, and other information held in NRS could be used in association with that description to identify the individual, then you should consider removing the description. Bear in mind that the proliferation of the internet has made it much easier for people to piece together

¹³ Give consideration to the context of the information. When assessing a finding aid you should not just look at the file or item level description, for example a name in an item level description might not appear to disclose information that has caused the item to be closed. However if the item is part of a collection, the very nature of which is sensitive, for example Outright Scotland (GD467), or Lothian Marriage Counselling Service (GD386), then the inclusion of the name in the description should be avoided.

information about individuals. If the records are closed, however, and the description does not identify the individual, then it is reasonable to include the personal data in the catalogue. For example a court case: Lord Advocate v Jones, where the papers are closed, does not identify the individual.¹⁴

- 9.5 *Is it really necessary to identify the individual?* - Consider why someone may want access to the records. Generally case files, such as court records or employee files, will need to be indexed by personal name, as most researchers will be looking for a particular person. Administrative records that have been selected because they contain policy or precedent papers usually do not require personal data in their catalogue description.
- 9.6 *Is the information already in the public domain?* - Information disclosed in open court is in the public domain.¹⁵ Consider also the nature of the record: is it fair to assume that the record was publicly available prior to deposit with NRS?¹⁶
- 9.7 *Is it likely that release of personal information in a description could cause substantial distress or substantial damage?* - According to guidance issued by The National Archives¹⁷, for substantial damage or distress to be caused, actual harm is required. TNA further instruct that substantial distress is less likely to be caused if the information has previously been in the public domain.
- 9.8 *Is this part of our duties under the Public Records Scotland Act 1937?* - We are charged under the 1937 act to retain records for historical purposes, and make “calendars, indexes and catalogues” of those records. Therefore if the records are public records defined in this act, and they are open, then we are carrying out our statutory duties of providing access to them through the preparation of finding aids. Therefore if it is necessary to include personal data in the description and they fall into this category, then it is reasonable for us to do so.
- 9.9 In general terms it is best to apply common sense in these matters and consider if the inclusion of the personal data is necessary and unlikely to cause substantial distress or damage.

¹⁴ Always err on the side of caution. Although the name of an individual might not necessarily identify the person, give some consideration to the nature of the name. For example, while the name John Smith is a very common name and it might be harder to identify the individual, someone with an unusual forename or surname might be easier to identify. If you are in any doubt, do not include the name.

¹⁵ With some court records it can be difficult to determine what information was disclosed in open court and what was not and therefore a general restriction on access may need to be applied.

¹⁶ Substantial distress is less likely to be caused if the information has previously been in the public domain, even if it has not been formally published. On this basis, records describing treacherous conduct in the Channel Islands during the wartime occupation have been released. See ‘Access to Public Records’ section 4.3.3, The National Archives (2001), s.4.3.3.

¹⁷ See Annex A: Definition of Substantial Damage and Distress.

- 9.10 If the records are open, public records that are case files, or exceed in date the lifetime of the subject, then it is reasonable to include the personal data in the description. If the records do not fall into these categories further consideration and a documented decision is required. However, please note that health records of a deceased person are exempt under section 38 of FOISA for a period of 100 years after the date of the last entry in the records.
- 9.11 Sensitive personal data – the rules for the processing of sensitive personal data are more stringent and so if the personal data in the description is sensitive, or indicates sensitivity, then the inclusion of the personal data in the description should be avoided.
- 9.12 Provenance information – it is vitally important to historical research that the researcher can gain an understanding of the provenance of the records from the catalogue description. Therefore the inclusion of depositor information is often necessary. However when including depositor information some consideration should be given about the best way to present it. Acceptable forms of names for inclusion in the catalogue include:
- Territorial designations: Peter Ogilvie-Wedderburn of Balindean
 - Individual names that cannot be associated with other identifying information: Miss V Jones
 - Ex officio title: the Estate Manager of Lennoxlove Estate
 - Nobility: The Duke of Hamilton
- 9.13 Depositor information that identifies the individual, particularly the address, should not be included in the public catalogue. Information such as this should be held in the 'Notes' field of the catalogue.

10. Security of Archives

- 10.1 All personal data must be stored securely to ensure that confidentiality is maintained at all times. Archives should be locked away in designated storage areas when not in use to prevent unauthorised third party access.

11. Access to Personal Data in Archives

11.1 Data Subject Access

Individuals are entitled to know what personal data NRS holds about them and to request a copy of this data in a form which is comprehensible. These requests are

known as subject access requests and must be processed within 40 calendar days. All requests must be submitted in writing and a copy of our *Subject Access Request Form* should be provided to the applicant to complete.

11.2 Research Access to Personal Data

Access to personal data contained in archival material by someone other than the data subject or data controller may be permitted for research purposes.

Section 33 of the Act allows records containing the personal data of identifiable living individuals to be used for historical or statistical research purposes provided that:

- the data are not processed to support measures or decisions with respect to particular individuals;
- the data are not processed in such a way that substantial damage or distress is, or is likely to be, caused to any data subject.

The Act therefore permits researchers to use personal data accessed in the NRS search rooms provided they abide by these conditions and nos. 1, 3, 4, 6, 7 and 8 of the Data Protection Principles.

11.3 Research Access to Sensitive Personal Data

The Data Protection (Processing of Sensitive Personal Data) Order 2000 provides the circumstances in which such sensitive personal data may be processed. Paragraph 9 allows processing for research purposes provided this:

- is in the substantial public interest;
- is not used to support measures or decisions about an individual without their explicit consent;
- does not cause, nor is likely to cause, substantial damage or distress to any person.

In order to protect the privacy of the individuals concerned, archival material of this nature is generally closed to public access for the lifetime of the individual. In some circumstances, however, NRS will provide access to sensitive personal data in its collections for research purposes. Researchers wishing to consult closed archival collections which contain sensitive personal data should complete an 'Application to Consult Sensitive Personal Data' form available from the search room supervisor. On receipt of the application, a judgement on access will be reached based on the sensitivity and nature of the personal data involved. The access assessment will be

made by the data controller and, if possible, the record creator. If an application is rejected, a full summary of the decision will be sent to the applicant.

11.4 Access Arrangements for Particular Records

Specific access arrangements have been agreed with the depositors of the following records:

11.4.1 *Crown Office and Procurator Fiscal's Office (AD)*: Requests for access to case records of Crown Office and Procurator Fiscal's Office (COPFS) to which access has been restricted should be referred to COPFS, which will make a decision on access. Crown Office, 25 Chambers Street, Edinburgh EH1 1LA.

11.4.2 *Court of Session (CS)*: Access to the vast bulk of Court of Session records is unrestricted. However, access is restricted to certain classes of record either because they are likely to contain sensitive personal data or because a Court order has been placed upon them (e.g. in cases involving confidential commercial information). The NRS catalogue indicates where restrictions apply. Staff in the NRS search room are not permitted to produce any restricted records to researchers until they have obtained written consent from the Court of Session. This consent should be shown to the search room supervisor upon request. This procedure applies to all persons seeking access, including the police and officials from other courts or government bodies. Requests to view restricted Court of Session papers should be directed to: Office Manager, Court of Session, Parliament House, Parliament Square, Edinburgh EH1 1RQ.

11.4.3 *Sheriff Court Records (SC)* Criminal and family records in the Sheriff Court Records group are closed to public access for 100 years. Those records affected include; Criminal Libels & Indictments, Records of Criminal Jury Trials, Juvenile Court Records, High Court Circuit Trials appearing before the Sheriff Court, Divorces, and Family actions relating to children, e.g. separation and aliment. In certain circumstances, access is permitted to these records, e.g. if an individual is the subject of the data or if a reader wishes to access the information for research purposes. All persons seeking access should be directed to contact the Scottish Courts Service (SCS) by email on csbenquiries@scotcourts.gov.uk. Alternatively, they can discuss their enquiry or request additional information by contacting the SCS on 0131 444 3464.

11.4.5 *Gifts and Deposits (GD)*: Some records in the gifts and deposits series are subject to restricted access. These include:

- Royal Scottish Society for Prevention of Cruelty to Children (GD409) - The Society's administrative records are closed for 30 years and case files or records containing confidential material relating to children for 100 years.

- Records of Dr Guthrie's Schools, Edinburgh (GD425) - Many of the schools' records are closed for 100 years. Individual closure dates are given in the catalogue.

11.4.6 *High Court of Justiciary (JC)*: Requests for access to records of the High Court of Justiciary that are less than 75 years old should be referred to the Court, which will make a decision on access. The contact details are: Justiciary Office Manager, High Court of Justiciary, Parliament House, Parliament Square, EH1 1RQ

11.4.7 *Mental Welfare Commission (MW)*: An arrangement has been agreed with the Mental Welfare Commission for Scotland for handling requests for access to their closed records. Researchers must complete a specific application form. Decisions on access are made by the Commission.

11.4.8 *Scottish Government Files*: The Scottish Ministers are data controller for information held in Scottish Government files transferred to NRS. Where the Scottish Government receives a data subject request which may involve information transferred to NRS, Government Records Branch (GRB) will check the NRS catalogue of files to ascertain if the data subject's name appears and inform the SG Data Protection Team of the outcome in time to allow them to reply to the enquirer within 40 days. If NRS receives a data subject request for information which may be held in transferred files and which are not yet publicly available, it will inform the requester that their enquiry has been referred to the SG Data Protection Team. In such cases, GRB will check its catalogue of files to ascertain if the data subject is mentioned and forward the results to ISIS along with the original request. If a requester's name does not appear in NRS's catalogue of transferred files, but the SG Data Protection Team feels that a more detailed search of the files is required, the Team will request the temporary retransmission of the relevant files in accordance with the service level agreement. Where NRS receives a request for personal information held in transferred files which are already open to the public, NRS will deal with the request in accordance with its normal public search room procedures without referring it to the SG Data Protection Team.

11.5 **Search Room Users**

All users of NRS search rooms must be issued with a reader's ticket before they are allowed to consult records.

Search room staff should issue new readers with a copy of our fact sheet *Research Use of Personal Data in National Records of Scotland*. This fact sheet provides guidance on research access to personal data contained in archival records and explains the responsibilities of researchers using such data in the course of their research at NRS. The fact sheet offers practical guidance only. It does not represent legal advice nor is it a substitute for it.

Search Room staff should draw readers' attention to the responsibilities outlined in this fact sheet and remind them that by signing the declaration at the bottom of the reader's ticket form they are undertaking to abide by these terms of access and use.

11.6 **Responding to research enquiries outside European Economic Area (EEA)**

Principle 8 of the Act states that personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Information Commissioner considers the transfer of personal information to countries outside the EEA acceptable provided that the information is lawfully open for research on an unconditional basis and its disclosure will not adversely affect the data subjects.

Where archives are generally closed and made available to researchers on a conditional basis then their transfer outside can only be justified provided adequate safeguards are taken to protect the rights and freedoms of data subjects. The researcher signing the '*Data Protection Declaration*' undertaking to abide by the conditions of access and use outline in 'Research Use of Personal Data in National Records of Scotland' should ordinarily satisfy this requirement.

11.7 **Archives on the Web**

Archives containing personal information relating to living or potentially living data subjects should only be placed on a website if publication will not cause substantial damage or distress to the data subjects. As a general rule, personal data that is not already in the public domain should not be placed on Web pages without the consent of the data subject.

Archives under consideration for publication online should be checked to ensure that either (a) the information concerned refers only to deceased data subjects or (b) disclosure via this media will not cause substantial damage or distress to the data subjects.

11.8 **Other Third Party Access**

Requests for other third party access should be referred to the Records Manager.

Annex A: Definition of Substantial Damage and Distress

Extracted from 'Access to Public Records' section 4.3.3, The National Archives (2001).

Extended closure should be applied to protect sensitive personal information about individuals, the disclosure of which would cause substantial damage or distress to the person affected by disclosure. The definition of substantial distress is clearly of central importance here. Both adjective and noun need to be considered carefully. The test is not one of mere embarrassment or discomfort, but distress and the level of distress required was raised in 1993 by the addition of the qualifying adjective. Nor is substantial distress alone sufficient, actual harm is also required.

Records should be considered for closure when they include medical case histories, especially when they reveal details of mental illness or socially stigmatised illness (e.g. bowel problems, infertility or impotence, mental illness or certain cancers). Records describing unusual sexual behaviour (e.g. promiscuity, masochism or frigidity) have also been made subject to extended closure. Records containing information regarding homosexuality should be considered on an individual basis. Although homosexuality has won much wider social acceptance, and some homosexual acts are now legal, this may not have been the case at the date of the record. Substantial distress may still arise from such releases and each case needs to be assessed carefully and documented.

Substantial distress is less likely to be caused if the information has previously been in the public domain, even if it has not been formally published. On this basis, records describing treacherous conduct in the Channel Islands during the wartime occupation have been released. The behaviour of those described in the records was widely known in the community.

Records, the disclosures of which would reflect badly on an individual's professional competence or the conduct of their job should not be closed for an extended period. Equally comments on an individual's character or morality need to be of a profound nature if they are to merit extended closure. Again, a judgement needs to be made of the circumstances of a case; observations on the dishonesty of a convicted fraudster may be appropriately opened whereas the same observations about a priest, might cause substantial damage and result in actual harm and therefore rightly remain closed. In each case it must also be established that actual harm would be caused by release.

Annex B: Depositor Questionnaire

NRS DEPOSITOR QUESTIONNAIRE	
1	Does the collection contain personal data already covered by a notification to the Information Commissioner? If so, obtain details of the notification.
2	Are any personal data exempt from subject access?
3	Does the deposit include any sensitive personal data as defined by the act? If so specify the category of sensitive personal data.
4	Discuss and agree with the depositor the data protection role to be assumed by NRS.