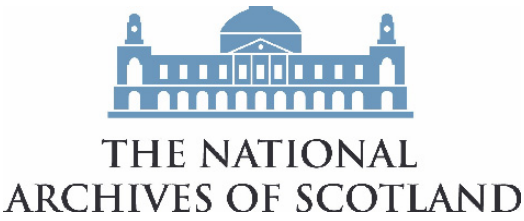

DATA PROTECTION CODE OF PRACTICE ON ADMINISTRATIVE INFORMATION

Contents

1. Introduction

The National Archives of Scotland is required by law to comply with the Data Protection Act 1998, which was enacted to ensure the fair and lawful processing of personal data. This code of practice has been drawn up to ensure NAS complies with the legislation by following corporate wide policies and procedures for the management and administration of information created or received by us in the course of our business transactions. This code applies solely to NAS corporate information. It does not apply to archival information transferred to NAS for permanent preservation, which will be the subject of a separate code of practice.

NAS 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 NAS Data Protection Policy adopted in March 2002. This requires every member of staff to familiarise themselves with and follow NAS data protection policy, guidance and practices, of which this code forms a part.

The National Archives, the Society of Archivists, the 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 publication provides wider guidance on data protection issues as they relate to archivists and records managers and staff are advised to consult this as appropriate. The NAS Code of Practice on Administrative Information draws on this code and complements it by detailing the specific policies and procedures to be followed within NAS.

If after reading this document you are unsure about any aspect of data protection you should contact the NAS Data Protection Officer for further guidance.

2. Roles and Responsibilities

2.1 Corporate Responsibility

The Keeper of the Records of Scotland as data controller for The National Archives of Scotland has primary responsibility for ensuring that all collection and processing of personal data within NAS complies with the Data Protection Act 1998 and the principles identified therein.

The Keeper has appointed a Data Protection Officer to act on his behalf to oversee compliance.

All NAS staff are responsible for ensuring that they comply with the principles set out in the NAS Data Protection Policy and any specific duties which relate to data protection should be incorporated into job descriptions.

The NAS Data Protection Policy is subject to regular review by the Management Board, who will investigate modifications when necessary.

2.2 Particular Roles and Responsibilities

All staff

- familiarise themselves with and follow the NAS Data Protection Policy and practices
- ensure that procedures for the collection and use of personal data are complied with in their area
- familiarise themselves with the implications of data protection in their job

Line Managers

- ensure staff with specific data protection responsibilities have these written into their job descriptions
- ensure staff with specific data protection responsibilities fulfil these properly
- ensure all staff receive data protection training provided

Data Protection Officer

- ensures that the NAS Data Protection Notification is kept up to date
- ensures all staff are familiar with NAS Data Protection Policy and procedures
- supports all staff to ensure they comply with their obligations under the Act

- provides guidance and training
- monitors the proper functioning of data protection systems

3. Data Protection Principles

The Act requires organisations and individuals who handle personal information to comply with eight data protection principles:

1. 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 is met, and

   in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. 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.
8. 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 and freedoms of data subjects in relation to the processing of personal data.

4. Defintions of Personal Data and Sensitive Personal Data

Under section 1(1) of the Act “data” are defined as information processed or recorded in specified ways.

4.1 Personal Data

“Personal data” are defined as data which relate to a living individual who can be identified –

(a) from those data, or

(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.

4.2 Sensitive Personal Data

Stricter conditions apply to the processing of 'sensitive personal data'. Under section 2 of the Act “sensitive personal data” are defined as personal data consisting of information as to –

(a) the racial or ethnic origin of the data subject

(b) his political opinions

(c) his religious beliefs or other beliefs of a similar nature

(d) whether he is a member of a trade union

(e) his physical or mental health or condition

(f) his sexual life

(g) the commission or alleged commission by him of any offence

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

5. Collection and Processing of Personal Data

In the course of our business transactions we will collect and process various sets of personal and sensitive personal data. The Act, and the principles therein, is designed to ensure that these data are accurate, up-to-date and processed correctly.

When you are collecting personal data, whether from clients, customers or colleagues, you should always carefully consider why the information is being collected and what you are going to do with it. At all times your approach should be to question the relevance of the data being collected. Each piece of personal data requested for processing must be relevant to the processing it supports. Excessive or irrelevant data cannot be collected.

When collecting personal and sensitive personal data, staff should always take time to explain to the data subject their rights under the Data Protection Act. Data subjects have the right to be informed of the identity of the data controller and the intended purposes of processing. Anyone collecting personal data should be open about why they are doing so and how they intend to use the data.

If you are going to begin a new process which requires the collection of personal data you should always consult the Data Protection Officer first.

5.1 Justifications for Collection and Processing

Any collection and processing of personal data must be justified by one of the conditions set out in Schedule 2 of the Act. The conditions that may be applicable in NAS are:

- The data subject has given their consent
- The processing is necessary for the performance of a contract with the data subject or for taking steps at the data subject's request to enter into a contract
- The processing is necessary to ensure compliance with any legal obligation other than that imposed by a contract
- The processing is necessary to protect the vital interests of the data subject
- The processing is necessary for the administration of justice, for the exercise of any functions conferred by any Act, for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or for the exercise of any other functions of a public nature in the public interest
- The processing is necessary for the legitimate interests of the data controller or third party recipients providing it is not prejudicial to the rights and legitimate interests of the data subject

And any collection and processing of sensitive personal data must be further justified by one of the conditions set out in Schedule 3 of the Act. The conditions that may be applicable in NAS are:

- The data subject has given their explicit consent to the processing
- The processing is necessary to meet legal rights or obligations in connection with employment
- The processing is necessary to protect the vital interests of the data subject or another person where consent cannot be obtained
- The information in the personal data has been made public as a result of the deliberate actions of the data subject
- The processing is necessary for legal proceedings, obtaining legal advice, or otherwise establishing, exercising or defending legal rights
- The processing is necessary for the administration of justice, for the exercise of any functions conferred by any Act, for the exercise of any functions of the Crown, a Minister of the Crown or a government department
- The processing is necessary for medical purposes carried out by a health professional or a person who owes an equivalent duty of confidentiality
- The processing is of personal data relating to racial and ethnic origin and is necessary to monitor and promote equality of opportunity
- The processing is in circumstances specified by an order of the Secretary of State

These conditions do not need to be met when processing category (e) personal data, that is, relatively structured or unstructured data held by a public authority.

5.2 Good Data Collection Checklist

Any form used to collect personal data within NAS should provide the person contributing the data with:

1) The identity and address of the data controller. This will always be:

   The Keeper of the Records of Scotland
   The National Archives of Scotland
   HM General Register House
   2 Princes Street
   Edinburgh
   EH1 3YY

2) A brief description of the purposes for which the data will be used.

3) Details of any third parties to whom the data will be disclosed and the opportunity for the data subject to indicate if they consent or dissent.

4) Notice that it is intended to transfer the data outside the European Economic Area (EEA) and the opportunity for the data subject to indicate if they consent or dissent. If you do intend to send data outside the EEA you should always consult the Data Protection Officer first.

5) Details of how to seek access to the data and correct any inaccuracies in it.

This information should be written clearly in plain English and prominently placed on the data collection form. A sample copy of the data collection form should be retained for as long as the data itself is retained.

Standard text which should be included on data collection forms concerning data subject rights and non-disclosure to third parties is provided in Annex A.

5.2 Consent

The data subject must always provide consent to the processing of their personal data. This consent must result from active communication and cannot be inferred from a failure to respond. Any paper form used to collect personal data should contain an area for the subject to sign to indicate consent. Where data are obtained electronically the data subject should be provided with a privacy statement explaining the intended use of personal data and be required to acknowledge this and their consent via a checkbox before the data can be submitted (see section 10 on NAS websites).

5.3 Disclosure to Third Parties

There are very few instances were we would disclose personal data to third parties without the data subject's prior consent. Consent should usually always be sought first by referring requests for personal data to the data subject directly. One exception would be to respond to an urgent request from a confirmed, reliable source, when the data subject's consent cannot be obtained and disclosure is necessary to protect the 'vital interests' of the data subject. The Information Commissioner considers 'vital interests' to be matters of life and death.

Consent can be set aside only if any delay will endanger the health and welfare of the data subject, their dependants or that of another person where this is dependant on the disclosure. We should give consideration to the balance of benefit and harm arising from disclosure. A significant gain to a third party can outweigh a minor inconvenience to a data subject. A judgement should be formed as to the reasonableness of disclosing the data according to the circumstances. A medical emergency or some other time critical event could meet the criteria.

We must be sure that the third party is trustworthy and that there exists an urgent need for disclosure. Not all requests may be honest. Some can be invasive or a risk to personal safety and security. Legitimate requests frequently originate from organisations, family matters being an exception.

Official requestors will respect your caution. They should be similarly aware of the need to protect personal data and are likely to operate similar procedures in their own place of employment.

We should keep a record of third party requests for personal data and of any disclosures made without consent and inform data subjects of these.

For information on disclosure of CCTV footage see section 11.

5.4 How do we handle calls?

When obtaining or giving out personal data over the telephone staff should be careful to request or supply only relevant information.

For example you should not take a caller's address unless you intend to visit or send something to that address.

We can supply names, work numbers and responsibilities from the staff directory or put callers through to staff and work areas directly. We should not disclose work locations to protect staff going from and to their workplace. We should not disclose personal information such as home phone numbers, addresses or work locations to third parties. Instead we should request the caller's contact details to pass on so that staff can respond personally.

6. Notification

Notification is the process by which a data controller informs the Information Commissioner of certain details concerning their processing of personal information in order to ensure openess. The Keeper of the Records of Scotland is legally required to notify details of all processing operations that involve personal data to the Information Commissioner's Office (ICO). Failure to notify is a criminal offence.

The notification provides a general description of the processing of personal data including:

- The purposes of processing
- A description of the data subjects
- A description of the data classes
- A list of recipients
- Information about whether the data are to be transferred outside the EEA
- Statements concerning security arrangements

Notification is renewed annually and any amendments should be made as required. When any part of our entry becomes inaccurate or incomplete we must inform the ICO as soon as practicable and in any event within 28 days. The Data Protection Officer is responsible for updating our notification. The NAS notification can be viewed both on the public register available on the ICO website www.ico.gov.uk and on theOracle under Data Protection. If you conduct a process which is not mentioned on the notification you must contact the Data Protection Officer immediately so that he can update it.

Personal Data Auditing

In order to control the use of personal data within the office the Data Protection Officer will maintain an inventory of personal data systems to inform the annual renewal of our notification to the Information Commissioner. A personal data audit will be carried out annually to ensure the inventory is up-to-date.

Personal Data Audit Form

Any member of staff can complete a Personal Data Audit Form to notify the Data Protection Officer of any new processing being undertaken (see Annex C).

7. Subject Access Requests

7.1 Background

The Data Protection Act affords data subjects data certain rights including:

- right of access to inspect data held about them
- right to prevent processing of data
- right to sue for damage caused by wrongful processing

The most fundamental of these is the right to access. Data subjects are entitled to know what personal data an organisation holds about them and to request a copy of this data in a form that is comprehensible. These requests are known as subject access requests and must be processed within forty days.

7.2 Data Subject Rights within NAS

Section 7 of the Act provides that individuals who request access to their data should:

- be informed whether or not they are the subject of any data being processed by NAS
- where data are being processed, be provided with an intelligible copy of the information held about them. This should be provided in a permanent form, unless the provision of the information in a permanent form would involve disproportionate effort i.e. the excessive volume of information would preclude production. Information can be given to the data subject in electronic form if they are agreeable to that arrangement.

Individuals also have a right to:

- a description of the personal data of which they are the data subject
- a description of the purposes for which the data are being processed or are to be processed; this is based on the notification of purposes supplied to the Information Commissioner (see section 6).
- a description of the recipients of the data; again this can be drawn from the notification
- any information available to NAS on the source of the applicant's data

- where an applicant specifically requests it, the logic involved in any fully automated data taking that has or may have a significant effect on the individual concerned

7.3 Handling Subject Access Requests

The Data Protection Officer will handle responses to all subject access requests unless other arrangements are in place.

All subject access requests must be submitted in writing. Anyone making an oral request should be asked to submit it in writing and a copy of our Subject Access Request Form should be provided for them to complete. The form is available on the NAS website or in hard copy from the Data Protection Officer and any of our search rooms. Completed forms should be sent directly to the Data Protection Officer. We may also receive written subject access requests in letters or emails. These should also be passed directly to the Data Protection Officer to process.

No personal information should ever be given out to a data subject over the telephone.

Subject access requests for access to personal information created and processed by NAS, which does not form part of our historical record collections, will be handled by the Data Protection Officer.

Subject access requests for access to personal information in any of our closed historical records will also be handled in the first instance by the NAS Data Protection Officer. The NAS operates different arrangements with various depositors. Search room and listing branch staff may be required to provide assistance in identifying the data.

Subject access requests for access to personal data in open historical records should be referred to the search rooms and the enquirer will be provided with access to the records in accordance with the usual arrangements for readers or remote researchers.

NAS is legally required to provide this information within 40 calendar days, so there should be no delay in the processing of requests.

The procedures which the Data Protection Officer follows in order to process subject access request are outlined in Annex D.

8. Managing Personal Data in Current Records and Emails

8.1 Security of Personal Data

When you are dealing with personal and sensitive personal data you have a duty to take steps to ensure the safety and security of the data and ensure that there is no unauthorised access to it. The Records Management Manual sets out the procedures all staff should follow when handling current paper files containing personal data. When files are in active storage and in use day to day, they must be stored in a designated storage facility. Each branch has a limited active file storage facility which is monitored by the Records Management Unit. All files should be stored in these cabinets during active storage so as to avoid unauthorised disclosure of personal data.

Staff should always use the corporate filing scheme and avoid the creation of separate personal filing systems which will also be subject to the Act, but not the NAS corporate retention schedule.

8.2 Restricted Markings on Files

NAS operates a restricted marking scheme for the management of sensitive data in our current filing system. If you are filing information which is classified as sensitive personal data you should ensure that the file has the appropriate security marking – RESTRICTED PERSONAL. This will ensure that the file is securely stored away in locked semi current storage in the Record Centre. If the file you plan to file sensitive personal data onto does not have the appropriate marking you should notify Records Management Unit and ask them to change the marking.

8.3 Security of Electronic Personal Data

Personal data should never be stored on the local hard drives of office desktop computers or laptops, which are not secure. Staff should instead use the appropriate corporate or personal workspace on network drives to which access is controlled.

Staff using laptops outside the office should not to leave them unattended and should exercise due care to prevent any unauthorised personnel from accessing personal data on NAS systems.

No personal data should be stored on memory sticks which are not encrypted.

8.3 Emails

Emails, both incoming and outgoing, are covered by the Act if one or other of the following criteria is met:

- The sender or recipient is identifiable, either through their email address or the content of the email, or

- The text of the email contains personal data, i.e. facts, opinions or intentions about identifiable living individuals

The Act applies to all individuals in NAS and their personal mailboxes and word processed documents as well as the data contained in the corporate records system.

Staff should be aware that their emails may be monitored for legitimate purposes – for answering subject access requests and ensuring compliance with the Act.

As best practice you should delete all emails that are not part of the corporate record or are required for other reasons as soon as they have ceased to be of use. Emails required for permanent preservation should be saved in the NAS Records Management System - they should either be printed and filed on the relevant paper file or saved in the relevant folder on the G:\ drive corporate workspace.

All staff should be familiar with the NAS Email Policy. Staff should pay particular attention to the sections covering the transmission of inaccurate personal data through the use of statements of opinion:

> "Email containing inaccurate information in the form of opinion or fact about an individual is in contravention of the Data Protection Act. This may result in legal action being taken against NAS or the person(s) sending the email message and anyone forwarding the email message to others."

8.4 NAS Remote Access System

The NAS Remote Access System allows authorised users remote access to the office email, theOracle and selected network drives. Users of the system should exercise due vigilance to ensure that their account and password details are not divulged. You should not leave an active connection unattended or allow anyone who is not an authorised member of NAS staff to access the office systems using your account.

8.5 Retention and Destruction of Personal Data

Personal data should not be retained for longer than it is required for the purpose for which it was collected.

Personal data for which a subject access request has been received must not be destroyed, altered or concealed to prevent disclosure. This does not preclude routine destruction as part of our records management programme.

9. Employee Personal Data

The Act is not intended to prevent employers from carrying out the legitimate needs of their business. There are obvious reasons why an employer needs to collect, retain and process personal data, whether for pay, pensions, sickness, absences or to promote good employment practice via employee development or the monitoring of gender, ethnicity, disability. The Act is there to ensure that this is done with due consideration to the rights of individuals.

9.1 Staff Information

In NAS most of our official personnel functions are conducted by the Scottish Government Human Resources and they keep appropriate records. Attendance management returns and staff performance appraisals are now recorded on the eHR system. However, we do still conduct staff monitoring and development meetings, records of which may be retained locally. All line managers should maintain a registered file about their employees in accordance with the NAS file plan. This file should be used for the retention of additional development material and any other appropriate information which cannot be recorded on eHR. This file will only be accessible to the member of staff featured in the data and their current line manager. All staff have a right to consult their file as and when they choose. They can do this by ordering out the file through the normal records management procedures. You do not have to lodge a formal subject access request.

9.2 Good Practice for Line Managers

- Ensure all staff are aware of all information which will be kept about them, how it will be used and to whom it will be made available
- Ensure staff are made aware of their rights under the Act (at least informing them generally of the Act's provisions) including the right of access to information kept about them
- Any relevant employee personal data should be retained on registered corporate files
- Electronic copies should be deleted once a hard copy has been produced
- All personnel restricted files should be kept in secure storage

10. NAS Websites

All our websites should display a privacy statement which sets out how we collect, use and store personal information gathered through the websites. The statement should cover any automated collection of personal information about virtual visitors by the use cookies, log files or tracking interfaces such as Google Analytics.

If we collect personal data via online forms on our websites then the data subject should be provided with a privacy statement explaining the intended use of their personal data and be required to acknowledge this and their consent via a checkbox before the data can be submitted.

Any personal data gathered through a website must be transmitted and stored securely. Personal data should not be displayed on any web page.

On each occasion where personal data is exchanged via the website a link to the privacy statement should also appear to remind the data subject that they are passing on their personal data.

For a copy of the privacy statement which can be used on NAS websites see Annex B.

11. CCTV

The images captured and recorded by closed circuit television cameras are classed under the Act as information processed by 'equipment operating automatically' and as such are covered by legally enforceable information handling standards. NAS must therefore employ a number of procedures and document them in order to be compliant with the Act.

11.1 Purpose

We operate CCTV cameras in each of its three buildings, both inside and outside of the buildings, in order to prevent crime, to detect, apprehend and prosecute offenders, and to protect staff and property.

11.2 Documentation

The CCTV Procedures Manual provides guidance on the CCTV system used in NAS and its day to day operation. A CCTV Administration spreadsheet on the G drive is used to record the use of tapes, their degaussing and any access to and disclosure of images. Operating procedures are regularly audited by the Records Management Unit to ensure compliance with the standards outlined in the CCTV Code of Practice issued by the Information Commissioner.

11.4 Accessing Images

The images recorded by the CCTV cameras are being collected and monitored in order to prevent crime and uphold public safety. Staff with responsibility for monitoring the images recorded by the CCTV should only use the cameras for these purposes. Access to the images recorded on the CCTV tapes is restricted to authorised members of staff. To ensure the equipment and tapes are in good working order and images are being recorded accurately the Accommodation Assistant responsible for degaussing of the tapes in each area should check a sample of recorded images prior to degaussing.

11.5 Tape Security

Tapes should be stored in secure cabinets in the systems areas at General Register House and Thomas Thomson House, and in Room 10 at West Register House in. Viewing of tapes should take place in designated offices that afford privacy:

- GRH – Robertson Wing Conference Room.
- TTH – Security Room.

- WRH – Room 10. The footage in WRH is recorded on split screens and can only be viewed in that building.

A viewing log is kept on the CCTV Administration spreadsheet recording:

- Tape ID (system and code number): e.g. RED 1/1/2
- Date and time of viewing
- Names of persons viewing the images
- Reasons for viewing
- Outcome of viewing

11.6 Disclosure

Disclosure of recorded images to third parties and third party organisations should only be made in limited and prescribed circumstances. Third parties whom it may be acceptable to disclose to are:

- Law enforcement agencies where the images recorded would assist in a criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- The media, where it has been decided that the public's assistance is needed in order to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident
- People whose images have been recorded and retained and who have submitted a subject access request for a copy of the images

Any disclosures should be documented on the CCTV Administration spreadsheet recording:

- Tape ID (system and code number)
- Date and time of disclosure
- Identification of the third party to whom disclosure was made
- Reason for allowing disclosure
- The extent of the information disclosed

All disclosures must be authorised by the Data Protection Officer.

11.7 Editing of Images

If a request has been made for access to images which do not record any untoward event, it may be necessary to obscure the images of third parties who also appear in the images. We must consider whether the disclosure of images would represent an unfair intrusion into the privacy of the third party or cause unnecessary harm and distress.

If we cannot obscure images ourselves it may be necessary to contract the work to another organisation. A written contract specifying how the images may be processed must be drawn up with the contractor first.

12. NAS Contracts

The Keeper, as data controller for NAS, is responsible for the fair and lawful processing of all personal data subject to the provisions of the Act. If we employ any third party, whether an individual or company, to perform any task or service on our behalf which involves the processing of personal data, we must ensure that they also adhere to the provisions of the Act. This is best provided for in a written contract.

It is very important we do this as under the legislation it is the data controller, not the data processor who is directly obliged to comply with the Act. Therefore any breach of compliance, even solely by the data processor, would remain the responsibility of NAS.

A written contract serves NAS on two levels:

1. It provides compensatory recourse in the event of any breach of data protection legislation by the data processor

2. It ensures NAS is compliant with the legislation

NAS has two options for including Data Protection provisions in its contracts:

1. Amending all contracts to include personal data clauses as standard

2. Including a general statement in all contracts and attaching a data protection schedule to contracts, which involve the processing of personal data

The latter is the better option as it avoids unnecessary contractual burdens on activities that do not involve the use of personal data.

12.1 General Statement

The general statement should read:

“In cases where the contractor will be processing personal data on behalf of NAS, they will be expected to sign a supplementary contract to ensure compliance with the terms of the Data Protection Act 1998.”

12.2 Risks

If NAS does not hold data processors to a written contract we run the risk of exposure to severe penalties and risks:

- unlimited fine – imposed by Office of the Information Commissioner

- information notice – this could be served upon us, and would involve the external audit of NAS contractual practices, and court action against us
- severe embarrassment – any blunder involving non-compliance with an Act which is centred on records and record keeping issues would undermine our professional credibility

12.3 New Contracts

When we employ contractors to perform tasks for us we must assess whether these will involve any processing of personal data. Examples of data processing include:

- data imputing
- couriering
- internet service provision
- waste disposal
- cleaning which involves access to areas where data is held
- printing/publishing
- building work which involves access to areas where data is held
- disaster recovery

When personal data is passed to any third party this constitutes processing and disclosure. As the data controller we must ensure firstly that the processing is legal and compliant with the legislation and secondly that the data processor can also comply with the terms of the Act.

Before any new contract is negotiated the Data Protection Officer should be consulted to assess the data protection implications.

Any contractor who is selected to act as a data processor must offer sufficient assurances that they have appropriate measures in place to safeguard the personal data. All contractors should be assessed to ensure they can provide adequate security measures. In the case of sensitive personal data processing the security measures should be audited by NAS to ensure they are satisfactory.

12.4 Contractor Assessment Checklist

- All contractors should be assessed by NAS to ensure adequate security measures are in place using the Audit Security Questionnaire as a guide (see Annex E)

- NAS should conduct regular audits of data processors to ensure contractual obligations are met. This should be done by Finance and Administration Branch in collaboration with the Data Protection Officer

- All activities which use a third party contractor and involve the processing of personal data should be subject to a written contract in order to guarantee that the obligations under the Act of both NAS and the contractor are met

- The Data Protection Schedule should be added to any new contracts which involve the processing of personal data (see Annex F)

13. Further Guidance

The following websites contain further information about the Data Protection Act 1998 and its application:

Information Commissioner's Office (ICO) www.ico.gov.uk

CCTV Code of Practice 2008

Society of Archivists (SoA) www.archives.org.uk

Code of practice for archivists and records managers under Section 51(4) of the Data Protection Act 1998 (2007)

The National Archives www.nationalarchives.gov.uk

Data Protection 1998: A guide for records managers and archivists

Office of Public Sector Information (OPSI) www.opsi.gov.uk

Data Protection Act 1998

Ministry of Justice www.justice.gov.uk

Public sector data sharing: guidance on the law

ANNEX A

Standard Text for Data Collection Forms

All data collection forms should contain the following statement, unless the form is on an NAS website (see Annex B):

> ***Under the Data Protection Act you have the right to gain access to your personal data held by the National Archives of Scotland, by submitting a written request to the Data Protection Officer, at the address above/below. In order to make this as quick and efficient as possible, we have created a Subject Access Request Form, which will be given to you on request by any of our staff. On receipt of all the information required to process this request, the NAS will endeavour to supply the requested information within forty days, as the legislation prescribes. In addition, if you think any of the information about you held by NAS is inaccurate, you should contact us as soon as possible so that we can correct it.***

The following statement should be included if data are not to be disclosed to third parties:

> ***The information which we hold about you is confidential and will only be disclosed outside the NAS***
>
> - ***At your request or with your consent***
> - ***To investigate or prevent crime***
> - ***If the law permits it or it is in the public interest.***
>
> ***Otherwise the information will not be disclosed to any other party or organisation and is maintained by NAS staff for the purposes outlined above and in accordance with NAS Data Protection Policy.***

ANNEX B

Privacy Statement for NAS Websites

Privacy Statement

The National Archives of Scotland (NAS) is displaying this privacy statement in order to demonstrate our formal commitment to privacy. This statement applies to the NAS website: www.nas.gov.uk.

This statement does not cover links within this site to other websites. You may be asked for personal information if you want to take advantage of specific services the NAS offers through the website, such as subscription to our website updates or other mailing services. We will only use the personal information you provide to deliver the services that you have requested, or for other related uses for which you have given your consent. We will not pass your information to third parties without your consent. It is entirely optional for you to participate in these services. The information you provide will only be used to support and improve your customer relationship.

If you wish to withdraw from any of the services which are operated through our website you can instruct us at any time to cease our processing and delete your personal information from our records. You also have the right to gain access to your personal data by submitting a written request to the NAS Data Protection Officer.

Use of 'Cookies'

When you visit the <*Name of Website*> website, we automatically send your computer a tiny text file called a 'cookie'. A cookie is a piece of information placed on your computer's hard disk that identifies your browser software to a website. By telling us who you are, it allows us to make your experience on the website a more personalised one and gives us more information as to how to make the site more useful to you. It also saves you from having to register and log in every time you use the website. As the website evolves, we will be able to provide you with additional levels of service based on our ability to recognise you via your cookie.

Our use of the cookie is limited to your activities within the website and does not have any other effect on your computer or your other activities on the Internet. <*Name of Website*> does not disclose information stored in your cookie to third parties. Users have the opportunity to set their computers to accept all cookies, to notify them when a cookie is issued, or not to receive cookies at any time. The last of these means that certain personalised services cannot then be provided to that user.

Use of Google Analytics

<*Name of Website*> uses Google Analytics to help analyse how users make use of our website. This is an analytical tool that makes use of 'cookies'. The information generated by the cookie about your use of the website, including your IP address, is transmitted to Google. This information is then used to evaluate visitors use of the website and to compile statistical reports on

website activity for us. <*Name of Website*> will not use or allow any third party to use Google Analytics to track or to collect any personally identifiable information of visitors to our website. We will not associate any data gathered from this website with any personally identifying information from any source as part of our use of the Google statistical analytics tool. Google will not associate your IP address with any other data held by Google. Neither <*Name of Website*> nor Google will link, or seek to link, an IP address with the identity of a computer user.

Changes to this statement

Due to changes in legislation and best practice or enhancements to functionality and content on <*website address*> we reserve the right to change our privacy policy and will reflect those changes in this statement.

ANNEX C

PERSONAL DATA AUDIT FORM FOR ADMINISTRATIVE INFORMATION

Branch responsible for data

«Branch»

Name of collection of personal data

«Name of collection»

Description (including dates of material)

«Description»

What is the nature of the personal data?

«Nature of data»

What is the data used for?

«Use»

Who/what is the source of the data?

«Source»

Where is the data stored?

«Storage»

Who has access to the data?

«Access»

What are the security arrangements?

«security arrangements»

How long is the data kept?

«Retention period »

Is the data seen or sent outside the EEA?

«EEA»

What uses and disclosure has the data subject agreed to?

«**Uses/Disclosure**»

Is the data regularly checked for accuracy?

«YES/NO»

When was it last checked?

«Date»

ANNEX D

Guide for Responding to Subject Access Requests

1. Step One: Logging Request

Any subject access request should be logged on the Online Central Enquiry System. Select “create a new Enquiry” and complete all the details. At the drop down list for enquiry type select Data Protection. This will ensure that you are notified by email when your request is nearing the date by which it should have been answered.

2. Step Two: Initial Check

The request should be checked to see whether enough information has been supplied for the personal data to be found. It may be necessary to reply to the data subject seeking more information before a search can be conducted. For example, it would be reasonable to expect former members of staff to give rough dates of employment, or members of the public to be able to clarify whether the personal data relate to them as readers, as conference participants, etc, or whether the data are contained within the archival records.

If an email address or a telephone number is supplied by the data subject try to use these to gain further information as this will provide the speediest response and will facilitate the expedition of the enquiry.

If no such contact information has been provided you must write to the data subject. You should place the enquiry on hold on the Central Enquiry System and note that further information was required.

3. Part Three: Verification and Validation

There is a duty on NAS to ensure that we disclose personal data only to the data subject or a chosen representative. We must therefore take steps to ensure the identity of the person making the request.

The NAS Data Protection Officer will undertake verification and validation. Verification is a check that the person making the request is the person they say they are. Validation is a check that this person is the same person as the one about whom the personal information is held.

Verification is done by checking any of the following forms of identification:

- passport
- national identity card
- driving licence (if it bears a signature that can be checked against the applicant’s)

As a general rule, the rigour of verification effort should depend on the sensitivity of the information requested. For postal requests copies are acceptable, but originals are preferred. A copy of the means of identification should be made and retained with the record of the request for access.

Validation is done by forming a judgement on the basis of the details supplied in the request and the nature of the information sought. With a well known person this will be straightforward, otherwise it is reasonable to make an assumption that the requester is the subject of the information unless there are reason to have doubts. A check of additional information supplied with the request and included in the data requested should be performed to see if corroborative information exists, for example the address of the requester may help to identify geographic location which can be matched to information contained in the requested data.

If the request comes from someone claiming to act on behalf of the data subject, they should not be provided with the information sought unless they can provide evidence of their right to obtain it in the form of a written authorisation signed by the data subject with some way of showing it is genuine (such as a copy of any of the items listed in the section on verification which can confirm the authenticity of the data subject's signature). Again the rigour of validation effort will depend on the sensitivity of the information requested.

4. Step Four: Finding the Data

Data contained within NAS administrative records – responsibility for locating this information will rest with the NAS Data Protection Officer.

Data contained within historical archival collections for which NAS has responsibility as data controller – responsibility for locating the information will rest primarily with the NAS Data Protection Officer, but additional assistance may be required from the branch responsible for the administration of the collection in question.

5. Step Five: Deciding Whether an Exemption can be Claimed

The Act and related secondary legislation carry a number of additional provisions in relation to subject access, including further exemptions.

Health Data

One of the most significant of the additional provisions is the duty imposed on NAS to consult an appropriate health professional before providing previously unreleased health data to an individual making a subject access request.

"Health data" is defined in very wide terms and includes all personal information relating to the physical or mental health or condition of the data subject. It covers not only detailed medical data but also more general types

of information, such as whether or not the data subject is a smoker or takes regular exercise. Such information would not just be found in health records, but also for example in personnel records.

Where the health information concerned was not originally supplied by the data subject or is unknown to them, the Act imposes a duty to consult an "appropriate health professional" before any data can be released. This prevents disclosure to the data subject of information that may be seriously harmful to either the data subject or another person.

Following consultation, disclosure should be made only if agreed to by the appropriate health professional. Where the health professional advises against disclosure, the data controller is permitted to withhold the information from the copy of data supplied to the individual making the request.

The duty to consult an appropriate official is onerous and can be costly to NAS (standard rates for GPs on NHS might be up to £100). It is therefore worth relying on those provisions within the order which allow exemption from the duty to consult.

No duty to consult will arise where:

- the data subject originally provided the data

- the data subject has already had access to the data

- an appropriate health professional has provided written consent to the disclosure of the information concerned and the disclosure is taking place within six months of this written agreement

Disproportionate Effort

It may not be necessary to supply a copy of personal data held in a permanent form where the supply of that data would involve disproportionate effort, although there may still be a requirement to grant access by other means.

The test of disproportionate effort can be tricky to apply but the Commissioner has issued guidance in this area and has explained that when deciding whether or not to supply information in a permanent form the following criteria should be taken into account:

- the nature of the data concerned and the likely effect on the individual if the data are not retrieved. Where the individual would be adversely affected by a decision to withhold the data an argument for disproportionate effort would be difficult to sustain

- the difficulty and expense involved in supplying data, although this should be weighed against the nature of the data being requested

- for backup data, if the non-live data do not differ materially from that held on a live system it would certainly be disproportionate effort to supply two copies of the same information

All decisions regarding the use of disproportionate effort should be documented on the Data Protection Policy file and the Subject Access Request file.

Information relating to third parties

Information contained within personal data relating to the data subject who has made the subject access request will often also contain information relating to other data subjects ("third parties"). Where the personal data relating to the applicant also identifies another individual, the applicant's right of access must be weighed against the other data subject's right to privacy.

In determining whether the data relating to another individual can be provided, a number of factors need to be considered:

- **Seeking consent**
  The first consideration by the data controller organisation should be to attempt, where practicable, to seek the consent of the third parties to the release of their data. Where data consent is obtained then the information can be released.

- **Balancing the interests of two data subjects**
  Obviously, in some cases it may be extremely impractical to even attempt to seek third party consent, for example where a record contains the details of multiple third parties. In such cases, or where consent has been sought but refused, NAS should only disclose the other parties' details where it is reasonable in all circumstances to do so. In other circumstances the information may be so significant and of such importance to the applicant that he or she should be allowed access despite the fact that the other individual has not consented to the release of his or her information. In such a case the release of even confidential information may be justified

- **Editing third party data**
  Where it is not reasonable to supply the third party data, i.e. the information is too sensitive or irrelevant to the enquiry, the information must be edited to remove any details that may lead to the identification of the third party. It is important to bear in mind that this editing must be applied to any information that might allow the data subject to infer the identify of the other party.

  Where the third party data are not to be provided to the data subject making the subject access request, the third party information should be redacted from the copy provided to the data subject with an explanation of the redaction.

6. Step Six: Providing Information in an Intelligible Form

Data subjects must be provided with a copy of the information in a comprehensible form. This means that it must be intelligible to them and not just the data controller. The use of jargon should be avoided or explained within the formal response and an explanation should be provided for abbreviations or codes contained within the information.

7. Step Seven: Replying to the Request

The formal response will be administered by the NAS Data Protection Officer. The response should provide information about complaints procedures if the applicant is not receiving everything they requested. The subject access requests response letter template should be used for the formal response.

The Data Protection Officer should issue the papers (letter and copies of any information) by recorded delivery or arrange for the personal collection of the papers.

8. Letter Templates

The following document templates should be used on all communications dealing with subject access requests.

The templates can be located on the GRB branch O drive.

SA1: Request for Information/ Verification of details

Dear [Applicant]

Thank you for your recent enquiry about access to data under the Data Protection Act 1998. In order that we can meet your request, we would be grateful if you could complete and sign the attached application form and return this to us together with proof of identity.

Upon receipt of your application form we will use the information supplied by you to search our files and systems for data relating to you. Our findings will be forwarded to you, by recorded delivery, within 40 days of the receipt of your application.

Yours sincerely,

Data Protection officer
The National Archives of Scotland

SA2: Acknowledgement

Dear [Applicant]

Thank you for returning the completed application form for access to your information under the 1998 Data Protection Act. We also acknowledge receipt of the information you have provided by way of proof of your identity.

Arrangements have been made to use the information supplied by you to search our files and systems for data relating to you. Our findings will be forwarded to you, by recorded delivery, on or before the dd/mm/yyyyy.

Yours sincerely,

Data Protection Officer
National Archives of Scotland

SA3: No relevant information found

Dear [Applicant]

Further to our letter of dd/mm/yyyy, we have now completed the search of our files and systems for data relating to you.

Based on the details supplied by you [on our application form], we can confirm that no information required to be supplied under the Data Protection Act 1998 has been identified.

We trust you are satisfied with our findings, however, please do not hesitate to contact us if you would like to discuss this further.

Yours sincerely,

Data Protection officer
National Archives of Scotland

SA4: Information enclosed

Dear [Applicant]

Further to our letter of dd/mm/yyyy, we have now completed the search of our files and systems for data relating to you.

Based on the information supplied by you [on our application form], the enclosed information has been traced [and transcribed into an easy to read format for your convenience].

Also enclosed are details about the purposes for which the enclosed information is processed, its source and any recipients to whom the information may have been disclosed.

We trust you are satisfied with our findings, however, please do not hesitate to contact us if you would like to discuss this further.

Yours sincerely,

Data Protection Officer
National Archives of Scotland

ANNEX E

Audit Security Questionnaire

A General Procurement	Evidence	Comments
1. Is the data processor a reputable organisation with an established customer base?		
2. Are references from other clients available?		
3. Have checks been made to ensure that the organisation is solvent?		
Organisational security		
1. Does the data processor have a data protection infrastructure in place?		
2. Has an individual been appointed to take control of data protection responsibilities for the data processor?		
3. Will this individual provide a contact point for data protection enquiries from NAS?		
4. Has the data processor put a data protection policy in place? If so request a copy		
5. Is there evidence that the policy is implemented?		
6. What evidence can the data processor provide to demonstrate that it takes reasonable steps to ensure the reliability of staff who have access to data?		
7. Do all staff with access to the data controlled by NAS receive adequate levels of training in data protection?		
8. Can the data processor demonstrate that a breach of data protection is a disciplinary offence within the organisation?		
9. Are organisational measures in place to restrict		

access to staff without authority to process the data?		
10. Are provisions in place with any sub-contractors used by the data processor to ensure that similar levels of protection can be guaranteed where the sub-contractor has access to the data?		
Technical Security		
1. Are the automated systems used protected by a level of technical security appropriate to the data held?		
2. Are technical measures in place to restrict access to systems holding personal data?		
3. Are technical measures in place to secure data during transit?		
4. Is data stored by the data processor's subcontractors? If so can the data processor ensure that adequate technical measures are put in place by the subcontractor?		
5 Can both the data processors and their subcontractors demonstrate that data are backed up on a daily basis and stored in a secure site?		
Physical Security		
1. Are the premises on which the data are to be held secure?		
2. Is access to those premises restricted?		
3. Are the premises subject to 24 hour security?		
4. Are the premises monitored by CCTV?		
5. Within the premises are the areas where the data are to be held secure?		

6. If the data are held on a non-automated system, is access still restricted – for example locked cabinets, clear desk policy?		
7. Are any copies of data, print outs, obsolete back ups, etc disposed of securely?		
8. Are obsolete hardware and software from which data could be discovered disposed of securely?		
9. Is there an auditable data retention and destruction policy?		

ANNEX F

Data Protection Schedule

THE NATIONAL ARCHIVES OF SCOTLAND DATA PROTECTION SCHEDULE

The Data Controller and the Data Processor HAVE AGREED on the following clauses('the Clauses') in order to adduce to adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data controller to the data processor of the personal data specified in Appendix 1.

1. DEFINITIONS

1.1 For the purposes of the Clauses:

'personal data'; means data which relate to a living individual who can be identified-
(a) from those data, or
(b) from those data and other information which is in the possession of, or likely to come into the possession of, the data controller, and 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

'sensitive personal data'; means personal data consisting of information as to –
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or sentence of any court in such proceedings;

'process/processing'; in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including –
(a) organisation, adaptation, or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data;

'Data Controller' means 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;

'Data Processor'; means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

'Data Subject'; means an individual who is the subject of personal data;

'supervisory authority'; means the Office of the Information Commissioner.

'The Act'; means the UK Data Protection Act 1998.

2. DETAILS OF TRANSFER

2.1 The details of transfer, and in particular the categories of personal data the purposes for which they are transferred, are specified in Appendix 1 which forms an integral part of the Clauses.

3. THIRD-PARTY BENEFICIARY CLAUSE

3.1 The data subjects can enforce this Clause, Clause 4(b), (c) and (d), Clause 5 (a), (b), (c) and (e), Clause 6 (1) and (2) and Clauses 7,9 and 11 as third party beneficiaries.

3.2 The parties do not object to the data subjects being represented by an association or other bodies if they so wish and if permitted by national law.

4. OBLIGATIONS OF THE DATA CONTROLLER

4.1 The data controller agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data by him,, has been and, up to the moment of transfer, will continue to be carried out in accordance with the relevant provisions of the Act.

(b) that if the transfer involves sensitive personal data the data subject has been informed or will be informed before the transfer that this data could be transmitted to a data processor.

(c) to make available to the data subjects upon request a copy of the Clauses; and

(d) to respond in reasonable time and to the extent reasonably possible to enquiries from the supervisory authority on the processing of the relevant personal data by the data processor and to any enquiries from the data subject concerning the processing of this personal data by the data processor.

5. OBLIGATIONS OF THE DATA PROCESSOR

5.1 The data processor agrees and warrants:

(a) that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract and that in the event of a change in that legislation which is likely to have substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data controller and to the supervisory authority where the data controller is established, in which case the data controller is entitled to suspend the transfer of data and/ or terminate the contract;

(b) to process the personal data in accordance with the mandatory data protection principles set out in Appendix 2;

(c) to deal promptly and properly with all reasonable inquiries from the data controller or the data subject relating to the processing of the personal data subject to the transfer and to cooperate with the competent supervisory authority in the course of all its inquiries and abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(d) at the request of the data controller to submit its data processing facilities for audit which shall be carried out by the data controller or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the data controller, where applicable , in agreement wit the supervisory authority;

(e) to make available to the data subject upon request a copy of the Clauses and indicate the office which handles complaints.

6. LIABILITY

6.1 The parties agree that a data subject who has suffered damage as a result of any violation of the provision referred to in Clause 3 is entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that neither of them is responsible for the violation of those provisions.

7.2 The data controller and the data processor agree that they will be jointly ad severally liable for damage to the data subject resulting from any violation referred to in paragraph 1. In the event of such a violation, the data subject may bring an action before a court against either the data controller or the data processor or both.

7. MEDIATION AND JURISDICTION

7.1 The parties agree that if there is a dispute between a data subject and either party which is not amicably resolved and the data subject invokes the third-party beneficiary provision in Clause 3, they accept the decision of the data subject:

(a) to refer the dispute to mediation by an independent person, or, where applicable , by the supervisory authority;

(b) to refer the dispute to the courts.

7.2 The parties agree that by agreement between a data subject and the relevant party a dispute can be referred to an arbitration boy, if that party is established in a country which has ratified the New York convention on enforcement or arbitration awards.

7.3 The parties agree that paragraphs 1 and 2 apply without prejudice to the data subject's substantive or procedural rights to seek remedies in accordance with the other provisions of national or international law

8. COOPERATION WITH SUPERVISORY AUTHROTIES

8.1 The parties agree to deposit a copy of this contract with the supervisory authority if it so requests.

9. TERMINATION OF THE CLAUSES

9.1 The parties agree that the termination of the clauses at any time, in any circumstance and for whatever reason does not exempt them from obligations and/or conditions under the Clauses as regards the processing of the data transferred.

10. VARIATION OF THE CONTRACT

10.1 The parties undertake not to vary or modify the terms of the clauses.

APPENDIX 1

To the standard contractual clauses

This appendix forms part of the clauses and must be completed and signed by the parties

Data Controller
The data controller is (specify your activities relevant to transfer)
……
……
……

Data Processor
The Data Processor is (specify your activities relevant o the transfer)
……
……
……

Data Subjects
The personal data transferred concern the following categories of data subject (be specific)
……
……
……

Purposes of transfer
The transfer is necessary for the following purposes (please specify)
……
……
……

Categories of data
The personal data transferred will fall within the following categories of data (please specify)
……
……
……

Sensitive data
The personal data transferred fall within the following categories of sensitive data (please specify)
……
……
……

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients, (please specify)
……
……
……

APPENDIX 2

To the standard contractual clauses

Mandatory data protection principles referred to in the first paragraphs of Clause 5(b)
These data protection principles should be read and interpreted in the light if the provisions (principles and interpretation of the principles) set out in Schedule 1, Parts I and II pf the Data Protection Act 1998.

(1) Personal Data shall be obtained fairly and lawfully.
(2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
(3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or those purposes for which they are processed.
(4) Personal data shall be accurate and, where necessary, kept up to date.
(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
(6) Personal data shall be processed in accordance with the rights of data subjects under this Act.
(7) 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.
(8) 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 and freedoms of the data subjects in relation to the processing of personal data.