

# PROCEDURES FOR HANDLING PERSONAL INFORMATION UNDER THE DATA PROTECTION ACT 1998

## Contents list

- [1 Scope of the procedures](#)
- [2 Managing personal data as records](#)
- [3 Obtaining personal data](#)
- [4 Holding and using personal data](#)
- [5 Keeping personal data accurate](#)
- [6 Retaining or destroying personal data](#)
- [7 Keeping personal data secure](#)
- [8 Passing on personal data to others](#)
- [9 Data subject access and other rights](#)
- [10 Third party access to personal data](#)
- [11 Sending personal data out of the country](#)
- [12 Personal data in the archives](#)
- [13 Further information and advice](#)
  
- [Annex 1 Definitions of data protection terms](#)
- [Annex 2 Frequently asked questions](#)
- [Annex 3 Report form for sets of personal data](#)
- [Annex 4 Data subject access request form](#)
- [Annex 5 Subject access requests – personal information about staff \(past and present\)](#)
- [Annex 6 Exemptions from data subject access rights](#)

(Procedures approved by Executive Team in December 2007)

# 1 SCOPE OF THE PROCEDURES

These procedures for the collection and handling of personal information should be read in conjunction with The National Archives' Data Protection Policy Statement issued by the Chief Executive in December 2007.

They apply to all personal information created or collected by all constituent parts of TNA and its staff in the course of their daily work, including personal information for which the Controller of HMSO is responsible. The information includes:

- the names and other details of those who hold readers' tickets, attend events here or serve on our advisory or consultative groups;
- the names and other details of those who correspond with us or provide details during telephone calls;
- the names and other details of individuals who obtain licences to re-use Crown Copyright Information
- mailing lists of all kinds, both those held for events or as part of our customer relations and those in personal mailboxes;
- information about contractors and suppliers of goods and services;
- information held by managers about their staff, such as performance management information;
- word processed documents, spreadsheets and databases which contain personal details such as names and addresses
- emails, where either the person sending or receiving is identifiable or the contents refer to identifiable people

Collectively this personal information is called '*personal data*' and the people it is about are called '*data subjects*'. The information is generally held in systems such as DORIS (reader information), Objective (our records management system), Outlook mailboxes, and the Single Customer Database and other specific databases 'owned' by Marketing and Communications and other Departments.

**The general rule to be followed is to handle and use information about other people as carefully as you would wish information about yourself to be handled and used. These procedures are an expansion of that general rule.**

The procedures apply also to some of our archival holdings – see section 12 for details.

Some definitions of terms used in these procedures – those that are italicised – are at Annex 1. The Data Protection Principles referred to in the procedures are set out in the companion Data Protection Policy Statement.

## **2 MANAGING PERSONAL DATA AS RECORDS**

Personal data created, obtained and held by staff as a result of their work are part of our corporate records. They are subject to the procedures and business rules governing the management of records outlined in our Corporate Records and Information Policy (in development) and supporting guidelines.

As a general rule, TNA's Records Manager, Richard Leonard, should be consulted about the retention and destruction of sets of personal data. However, it is the responsibility of each member of staff to ensure that:

- incoming and outgoing emails are either filed or deleted once the action to which they relate has taken place, if not earlier. Those which remain in a personal mailbox pending a final decision should be reviewed at regular intervals and either filed or deleted. All emails will be deleted from personal mailboxes by system action after 3 months
- the contents of personal folders should be reviewed at regular intervals. Any documents which should form part of our corporate record should be filed in Objective and anything no longer needed should be deleted.

## **3 OBTAINING PERSONAL DATA**

*This section sets out good practice to be followed when acquiring personal information, for example for a mailing list.*

### **3.1 Be selective**

Consider what personal information you **need** to collect to achieve your objective, keep a record of your decision and ensure that you collect only that information. Do not collect irrelevant information simply because it might be useful at some point in the future. Consider whether depersonalised or anonymous information would achieve the same result as information with a name attached. For example, does a feedback form or survey questionnaire really need the name of the person completing it?

### **3.2 Be open and honest**

Be as transparent and candid as possible when acquiring personal information from people. One method of ensuring this is to ensure that any form or screen used to obtain personal data includes the following:

- the identity of the *data controller*. Our name, in full as ‘The National Archives’, should appear somewhere.
- a brief description of the purposes for which the information will be used. This can be a phrase or sentence such as ‘This information will be used only to process your order’ or ‘This information will be used to send you details of future similar events’. If you intend to make any additional use of the information see [section 3.3](#).
- a brief description of any proposed disclosure of the information to third parties and, if so, an opportunity for the person to give or refuse consent to this (see [section 3.3](#) for details)
- a statement that people have the right of access to information about them and the right to seek its correction
- if the information is likely to be transferred out of the European Economic Area (the European Union countries plus Norway, Liechtenstein and Iceland), this should be stated

This is a ‘fair processing notice’ and must be reasonably intelligible, in reasonably prominent type, and in a reasonably prominent position on the relevant form or screen. It could be along the following lines:

‘The National Archives will use your personal details only for <purpose> and related purposes. We will keep it only for as long as required for this purpose unless you agree to let us add you to our mailing list. (TICK WHICH APPLIES: YES  NO  ). If you wish to be removed from our mailing list at any time please email <email address>’

If the information is being obtained during a telephone call, and there is any intention to use it for any further purpose, e.g. to add to a mailing list, the person must be informed and asked to consent to this.

### **3.3 State future intentions and obtain consent**

If you know or think you will want to keep the personal information and use it for a different purpose, e.g. to add the names and addresses of those who have bought publications or made a telephone enquiry to our Single Customer Database, or our e-Newsletter mailing list, tell them and obtain their consent first. You can do this by including a sentence like this on a form:

‘We may want to inform you of future publications and events. Please tick the box if you are willing for us to add you to our customer database and use your details for this purpose <box>’

or during a telephone conversation:

‘Would you like us to let you know of any future publications or events that might interest you? I can add your name to our customer database if so. We will only use the information for this purpose.’

If you intend to pass people's details to third parties, for example to another archives institution or a museum, where it will be added to another mailing list, tell them and obtain their consent. You can do this by including a sentence on a form such as

'We may want to share your information with interested parties, such as museums or military history publishers. Please tick the box if you are willing for us to do so <box>'

The same point should be made in telephone calls although not necessarily in these words. Consent or refusal should be recorded so that whoever receives the personal information for action can act accordingly.

It is good practice to ask people to opt-in to different use or disclosure rather than to opt-out from them. If you want to ask data subjects to opt-out rather than opt-in, consult the TNA Data Protection Officer first.

If the personal information is *sensitive personal data* you **must** include an opt-in rather than an opt-out box on the form or screen. With *sensitive personal data* consent must be active and you cannot infer consent from a failure to respond. You cannot assume consent just because people have not clearly refused it.

Retain the evidence of consent for as long as you keep the personal information.

### **3.4 Information obtained from third parties**

If you receive personal data about an individual from a third party, check whether the third party has been authorised by the individual to supply it and keep a record of the answer. If so, your obligation to inform the individual of the information may be waived. Check also how accurate the person providing the information believes it to be and, if there is doubt about accuracy, keep a record of this in case you have to reply to a subsequent complaint from the subject of the information.

### **3.5 Be careful in creating personal data**

Do not make adverse comments about individuals unless they are based on recorded facts and can be defended as accurate if challenged. Whenever you write anything about individuals, remember that they have a right to ask to see what is written about them ([see section 9](#)).

### **3.6 New sets of data**

If you are collecting a new set of data, complete a Personal Data Report Form (see [Annex 3](#)) and send to the Data Protection Officer (currently Susan Healy). This applies only when you are deliberately assembling contact or other details, for example a new mailing list for an event or a group of people

with the same research interest. It does not apply to personal mailboxes and contact lists maintained by individuals for occasional personal use.

## **4 HOLDING AND USING PERSONAL DATA**

*This section sets out good practice to be followed when processing personal information. Processing includes holding and storing as well as actively using.*

### **4.1 Be able to justify processing of personal information**

Processing must always be

- fair to the person the information is about
- lawful, i.e. not forbidden by law, and
- have an additional justification

The best additional justification is the consent of the data subject. If you do not have consent but you can link your processing to any of our objectives or targets in our current corporate and business plan, then you can assume that your processing is justified on the grounds that it is necessary for us to carry out our functions. If you do not have consent or cannot make this link but need to process personal data, consult the Data Protection Officer before you start processing.

### **4.2 Compatible processing**

Personal information should be used only for the purpose(s) for which it was obtained or for compatible purposes. For example, information collected for research purposes must not be used for marketing purposes unless the data subject has consented to this different use. ([See also 3.3](#))

### **4.3 Processing sensitive data**

You need to be particularly careful if you are processing *sensitive personal data*. As well as being fair to the person the information is about, and lawful, you must be able to justify use of the personal information against one of the justifications in [4.1](#), i.e. we have consent **or** processing is essential for carrying out our functions, **or** one of the following justifications applies:

- processing is lawfully required for employment purposes
- the information has already been made public by the person concerned
- processing is needed for legal proceedings, to obtain legal advice or to establish or defend legal rights
- processing is needed for ethnic monitoring
- processing is necessary to protect the vital interests of the data subject or another person and obtaining consent is not an option

- processing is necessary for research purposes, will not involve making decisions about the data subjects and is unlikely to cause them substantial damage or distress

If none of these justifications can be used but you do need to process personal data, consult the Data Protection Officer before you start processing.

## **5 KEEPING PERSONAL DATA ACCURATE**

*This section explains the importance of keeping personal information accurate and up to date and what you should do about correcting inaccurate information.*

### **5.1 Personal information should be accurate and up-to-date**

Any personal information that you are processing should be accurate and up-to-date. The difficulties of ensuring total accuracy are recognised and a realistic approach is adopted in the Act by requiring 'reasonable' steps to have been taken to ensure accuracy. A relevant factor is whether the person will be disadvantaged by your processing. The more this is likely, the more careful you should be about accuracy.

Keep a record of the procedures you adopt for checking the accuracy of the data you obtain and process.

### **5.2 Requests for correction of personal data**

People have the right to seek correction of personal information about themselves. If someone states that information about them is inaccurate and can provide evidence to support this, the correction should be made.

Depending on the nature of the information, it may be necessary to record the fact of the correction and retain the incorrect data. For example, a simple change of address may require no formal record of amendment but something more complex that could affect the rights of the person concerned should be recorded and the incorrect information previously used for decision-making should be retained. If you think there is any likelihood that you might need to refer to the previous version, or be asked when it was corrected, keep a record of the correction, for example by adding a note 'corrected on <the date>' and signing it, if it is a paper record, or by filing a note in Objective.

If the change requested is complicated, or relates to information that is in any way disadvantageous to the data subject or to information that is not in current use, consult the Data Protection Officer.

We do not correct data in the archives. If such a request is received, refer it to the Data Protection Officer.

### **5.3 Inform third parties of corrections to personal information**

If you are correcting personal information consider whether it might have been passed to another department of The National Archives and, if so, whether they should be informed of the correction. For example, if readers change their addresses for DORIS purposes, the details should be passed to Marketing and Communications so that the Single Customer Database and any other databases can be updated. Similarly, if Marketing and Communications staff receives notification that someone on their mailing lists has died, they should tell ARK so that the reader's ticket can be cancelled and DORIS updated.

If the information was disclosed to a third party some years ago for a specific purpose, for example in connection with a job application, then sending a correction is unlikely to be necessary. If in doubt, consult the Data Protection Officer.

## **6 RETAINING OR DESTROYING PERSONAL DATA**

*This section sets out the need to make decisions about keeping or destroying personal information and to implement those decisions.*

### **6.1 Make retention/destruction decisions**

As a general rule, do not keep personal information for longer than necessary. Unless you are retaining it as part of the corporate record, or you have a specific reason for keeping it, destroy or delete it when you no longer need it for the purpose for which it was obtained. This includes emails in personal or shared mailboxes, which should either be filed in Objective or deleted. It is particularly important that emails containing sensitive personal data, for example information about someone's health, are not kept in mailboxes indefinitely. (Note that emails that remain in mailboxes are deleted automatically after three months.)

If personal information is being kept for the corporate record, make sure it is included in disposal schedules agreed with TNA's Records Manager and that it is destroyed in accordance with normal application of such schedules.

### **6.2 Data selected for preservation**

If you are keeping personal information as archives, or potential archives, contact the Records Manager for advice.

## 7 KEEPING PERSONAL DATA SECURE

*This section gives some basic guidelines about the safekeeping of personal information. See also section 6 of TNA's Security Handbook and our policy on Handling Data and Information, both on Narnia .*

### 7.1 Store personal information securely

It is very important that personal information is stored securely and access restricted to those with a need or right to see it. This is particularly the case if *sensitive personal data* is involved, or sets of information about a number of people.

Make sure that personal information held by you is not disclosed either orally or in writing, whether accidentally or not, to any unauthorised third party by taking the following measures:

- do not leave paper copies of personal information where anyone else can access them. Keep manual personal records locked away securely
- if you hold personal information on your computer, do not leave it unattended without locking the computer; do this also if you have a visitor who should not see the information on your screen
- if the personal information is filed in Objective, set privileges so that it can be accessed only by those with a need and a right to see it.
- If the personal information is held outside Objective and is not common knowledge, use passwords to secure it

In general, follow the guidance in TNA's Security Handbook and the Handling Data and Information Policy, both on Narnia .

### 7.2 Transmit personal information securely

Ensure that transmission of information, whether internally or externally, is done with a level of security appropriate to the nature of the information.

If the information is being transmitted within The National Archives by physical means, such as in an envelope, ensure the envelope is sealed and alert the recipient to the fact that you have despatched it. If it is being transmitted by email, ensure the email is marked as confidential.

If personal information is being transmitted externally, e.g. to a contractor or partner institution, the following rules apply:

- ensure the transmission has been approved by a Director
- use technical means such as encryption for transmission
- if a password is required, send it separately

### **7.3 Phone calls**

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access, and check their identity
- If a phone call requires authorised disclosure of personal information but in circumstances that would lead to people sitting close to you overhearing it, move the phone conversation to a room where you can have privacy

See [section 9](#) for guidance on checking identity.

### **7.4 Avoid loss, unplanned destruction or damage**

Ensure that unauthorised or accidental access, alteration, disclosure, destruction or loss of significant sets of personal information is kept to a minimum and, if it happens, that you record the circumstances and report the incident to our Departmental Security Officer, who is the Director, Corporate Services and Finance.

### **7.5 Destroy information securely**

When deleting information held electronically, ensure that it is removed from the Recycle Bin. Destroy paper-based personal information only under secure conditions - shred it or use a Confidential Waste bag. Further advice on this is available from the Records Manager.

## **8 PASSING ON PERSONAL DATA TO OTHERS**

*This section explains precautions to take if passing personal data to another person or organisation.*

**8.1** Do not pass personal data to anyone outside The National Archives without having first obtained approval from either a Director or the Data Protection Officer.

**8.2** If personal data is being passed to someone outside The National Archives, follow the guidance at 7.2 and keep a record including:

- sufficient details of the information for it to be clearly identifiable subsequently
- the name of the person who has authorised it
- details of to whom it has been sent

- the date on which it was sent
- the means used to send it, e.g. encrypted USB stick

## 9 DATA SUBJECT ACCESS RIGHTS

*This section outlines the rights of data subjects and how to respond to them.*

### 9.1 Data subjects have certain access rights:

- to be told whether information about them is being processed
- to be given a description of the information and the purpose for which it is being processed and details of others to whom it is or has been disclosed
- to see the information in intelligible form
- to be told how it was obtained

**9.2** To be valid, requests must be **in writing**, either on a form such as at Annex 4 or in a letter or email. Anyone making an oral request should be asked to put it in writing and a copy of the form should be offered.

**9.3** Personal information should not be given out to a data subject over the telephone unless you have no doubts as their identity **and** the information is innocuous. Suggested ways of checking identity are in the FOI Procedures, numbers 28-30 but are intended for dealing with written requests. For telephone enquiries, check the requested information. If it seems innocuous and the enquirer is able to answer a question from it, provide the information, but if you have any doubts, ask the caller to put their enquiry in writing.

**9.4** The procedures for handling data subject access requests from members of the public are set out in the FOI Procedures. These procedures cover requests for information in both the archives and our corporate records. If in doubt, consult the Data Protection Officer.

**9.5** Special arrangements apply to requests by staff for their personnel records - see [Annex 5](#).

**9.6** See [12](#) for an explanation of how subject rights apply to the archives.

**9.7** See [5.2](#) for how to handle requests for correction of personal data.

## 10 THIRD PARTY ACCESS TO PERSONAL DATA

*This section explains that written requests should be handled as set out in the FOI procedures*

**10.1** There is no right of access to information about other people (3rd parties) in the Data Protection Act. However, the Freedom of Information Act provides a limited right of access to this information – limited by the need to comply with the Data Protection Principles and generally be fair to data subjects. See the FOI Procedures for how to handle requests by 3rd parties, which must be in writing. Standard letters and paragraphs to be used in replies are annexed to those procedures and must be used.

**10.2** However, common sense can be applied here. If someone telephones to ask for the name of a member of staff with a particular work responsibility because they have a business reason for contacting them, provide the name and business contact details unless there is a particular reason not to do so. If you have any doubts, take the caller's contact details and say that you will ask the staff member concerned to contact them. **Never** provide a home address or phone number.

## 11 SENDING PERSONAL DATA OUT OF THE COUNTRY

*This section provides alerts to problems with exporting personal information.*

**11.1** Except in response to a subject access request, do not transfer personal information about living individuals outside the European Economic Area (EU countries, Iceland, Liechtenstein and Norway) unless (i) the data subject has given consent or (ii) a contract is in place which provides equivalent protection of the rights of data subjects. For more information on the countries to which personal information can be exported, see: <http://www.informationcommissioner.gov.uk/eventual.aspx?id=1163>.

**11.2** Transfer means physically transporting the data overseas as well as providing people abroad with access to the information, for example, via the internet. We will not place on our website personal information about staff, other than names, email addresses and, in some circumstances, work responsibilities, without their consent.

**11.3** Catalogue descriptions should not be added to The Catalogue if they relate to identifiable living individuals and release through our website would place in the public domain information which should be withheld in order to protect the individual from substantial damage or distress, or from endangerment.

**11.4** As a general rule, archives should not be placed on our website if we believe that publication there would cause substantial damage or distress, or would endanger them. In any event, archives will not be placed on the website if any conditions as to use of the information apply; they must be available in our reading rooms unconditionally to be eligible for the website.

**11.5** If a researcher requests copies of archives that are available on a conditional basis, e.g. an undertaking as to their use must be signed, refer the request to the Data Protection Officer. Copies will be sent to addresses outside the European Economic Area only if the person placing the order explicitly undertakes to respect the rights of the data subject under the Data Protection Act. The copies must be accompanied by warnings as to the recipients' obligations under the Act.

## **12 SUBJECT RIGHTS TO PERSONAL DATA IN THE ARCHIVES**

*This section deals with special provisions applying to people seeking access to personal information about them in the archives.*

**12.1** The Data Protection Act applies in general to archives containing personal information about identifiable living individuals, both electronic archives and those in traditional formats such as files, bound volumes or indexes.

**12.2** Data subject access rights apply to archives covered by the Act but we will claim an exemption if the archives are closed to the public, under section 33(4) of the Act, on the grounds that

- the records are being processed in a way that does not reveal the names of data subjects; and
- this processing does not cause those data subjects substantial damage or distress; and
- the processing does not involve decision-making affecting the data subjects

**12.3** However, even when the exemption can be claimed, as a matter of policy we will respond when the applicant has a real need of the information in recognition of the fact that we are a public institution that should, where possible, provide information necessary for tax payers to claim their rights and entitlements. Such requests will be referred to the person in charge of Remote Enquiries on that day to assess whether the individual's rights or entitlements seem to be at stake, with a view to ensuring we do nothing to impede those rights and entitlements being claimed.

**12.4** We require sufficient information to locate the information from the applicant, either in their initial enquiry or in response to a request for such information.

**12.5** Any decision to disclose information in records not open to the public will take account of any other exemptions in the Data Protection Act and will include consultation with the relevant government department. This will be handled through the Access Manager in RMCD. Details of how to do this are set out in the FOI procedures. See [Annex 6](#) for information about exemptions in the Data Protection Act.

**12.6** The fixed fee of £10 applies only when we are meeting our statutory obligation to provide data subject access. Where an exemption is claimed but the request is being dealt with as a matter of policy, our normal research fees can apply.

**12.7** Special provisions apply to unstructured personal information. This is information which is not part of a set of information structured by reference to individuals or criteria relating to individuals, for example subject or policy files in which names occur incidentally. We are not obliged to handle a request unless the applicant describes the information he believes is held. Even then, if identifying and finding the information would cost more than the statutory cost limit of £600 we can refuse to handle the request. When, however, the applicant is willing to pay for any additional costs involved, we will assess whether the individual's rights and entitlements are at stake and take this into account when deciding whether or not to undertake the search.

**12.8** See the FOI procedures for how to deal with subject access requests. Standard letters or paragraphs should be used when replying to subject access requests.

**12.9** See also [Section 10](#) re 3<sup>rd</sup> party access to personal information, [section 11](#) re sending copies overseas and placing archives on the website, and [Annex 6](#) for an expansion of the policy set out in this section.

## **13 FURTHER INFORMATION AND ADVICE**

For further advice contact the Data Protection Officer, Susan Healy, on extension 2305.

February 2008

## ANNEX 1 DEFINITIONS

### Personal data

Information about a living individual who can be identified from that data, or from that data and other information that is in the possession of, or is likely to come into the possession of, the Data Controller. It includes opinions about the individual, and any indications of intentions in respect of that individual.

There are five categories of personal data which are managed in slightly different ways:

**(a) and (b) Automated data.** Personal information which (a) is being processed or (b) may be processed by equipment operating automatically in response to instructions

**(c) Manual data.** Personal information held in 'relevant filing systems', defined as: *'any set of information relating to individuals to the extent that the set is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible'*. Card indexes, files bearing individual names, and subject files where names have been indexed or are otherwise easily traced are clearly 'relevant'; casual references to individuals in subject files are not. 'Specific information' about an individual may be widely dispersed but if it can be retrieved readily it will constitute a 'set'.

**(d) 'Accessible record'.** Health record, education record or certain local authority social services or housing records.

**(e) All other personal information** was brought within the scope of the Act from January 2005

### Sensitive personal data

Information relating to a data subject's:

- racial or ethnic origin
- political opinions
- religious or other similar beliefs
- membership of a trade union
- physical or mental health or condition
- sexual life
- (alleged) commission of any offence
- court proceedings for any (alleged) offence

### Data controller

The person or body responsible for deciding what personal information is obtained and how it is to be used. The National Archives is data controller for the generality of personal information held by it or processed under its instructions but the Controller of HMSO is data controller for personal information specific to administration of Crown Copyright.

**Data subject**

The person the information is about.

**Data Protection Officer**

The person within The National Archives who takes the lead on providing advice and guidance on all aspects of data protection.

**Processing**

Anything that can be done to personal data, from collection to destruction, and including use and also storage without use.

## **ANNEX 2 FREQUENTLY ASKED QUESTIONS**

### **What is the Data Protection Act about?**

The Data Protection Act 1998 ('the Act') ensures that any organisation that collects or holds information about living individuals does so in a way that is fair to that person. It does this by setting out 8 principles for the processing of personal data which organisations must work to (see the Data Protection Policy Statement for a list of the data protection principles). The Act also gives individuals rights of access to their own information, and prevents abuse of personal information by third parties.

### **Is The National Archives subject to the Data Protection Act?**

All organisations, whether public or private, large or small, must process personal information in accordance with the Act. The National Archives processes a variety of personal information. Our corporate information contains information about visitors and our staff and others with whom we have dealings, such as journalists and contractors. The archives themselves also contain personal information; see section 12 or Annex 6 for further details about personal information in the archives.

### **What personal information is covered?**

All recorded personal information should be processed in accordance with the Act. This means all written documents, whether in electronic or paper format, and information contained in other recorded media – CCTV footage or other video, audio cassettes and so on are also covered. The information does not have to be factual; opinions about a person are also included in the definition of personal data.

### **What are my rights as a data subject?**

The Data Protection Act gives individuals the right to know whether an organisation is processing personal information about them. If personal information is being processed, the individual has a right to know what information is being processed, how, and what for. They also have a right to see the data in an intelligible form; this will usually mean providing a copy of the information. People asking for this information are making Subject Access Requests. The Data Protection Act also gives people the right to correct inaccurate information about themselves.

### **How do I exercise these rights?**

By making a subject access request. Any person can make a subject access request; by writing to an organisation, asking to know what personal information is held, and what use is made of the information. To correct false information, you should write to the organisation pointing out the error, and where necessary, provide evidence that the information is incorrect. See Annex 5 to the Data Protection Procedures for how current staff can make subject access requests for their personnel files and other records.

### **Is there a charge for making a Subject Access Request?**

There is a fixed fee of £10 for making a Subject Access Request. This fee is generally waived for current members of staff seeking access to their personnel file.

### **I am collecting personal information as part of my job - what do I need to do?**

Only collect information which you really need and make sure that the person supplying the information knows how you intend to use it. If you intend to add their details to one of our databases, such as the Single Customer Database, make sure they are given an opportunity to agree or disagree. Don't then use the information for any other purpose. This applies whether you are collecting the information on a form, over the telephone, or via the website or email.

For full details, see the Data Protection Procedures, 3.1-3.3 and 4.1

### **What is sensitive personal data?**

is information that is considered particularly personal and private and therefore is given extra protection. The category includes details of religious and political beliefs, Trade Union membership, health, sex life, and prosecution for offences.

### **How should personal information be stored?**

Carefully! Keeping personal information secure and ensuring only those with a rights or need of access can see it is a very important part of the Data Protection Act.

### **How long can I keep personal information?**

As long as you need it – but you do need to have a continuing need of it and should not keep it just in case it might come in useful some day.

### **Can I give out personal information over the phone?**

Only with great care – consider the nature of the information and ensure the person on the phone is the one with a right of access.

### **Why do I have to keep track of sets of personal data?**

Each year The National Archives has to send a notification to the Information Commissioner of what sort of processing of personal data we are undertaking, so we need to know what we have and how we use it.

### **Can we still use Mailing Lists which were created on an 'opt out' basis?**

Only in exceptional circumstances – consult the Data Protection Officer.

### **Can two or more Mailing Lists be merged?**

You can merge two mailing lists which were both created on an 'opt in' basis for similar purposes. If you are unsure whether an individual chose to receive mail from us, or if the purpose of the new list is very different from the original list, then consult the Data Protection Officer.

**Can personal data be shared internally between departments?**

You can share personal information with another department if it is to be used for a purpose that is similar to the purpose for which the information was originally collected. For example, if a recipient of direct marketing informs us of a change of address, we can alter the address associated with his/her reader's ticket. But, unless the reader has given consent, we cannot use a record of which documents he/she has ordered as an indication of his/her interests and then send publicity about forthcoming publications which the shop will be stocking because that would count as a different use.

**Can we share personal data with external companies?**

We share personal data with other bodies only if the person has consented to this through a specific 'opt in' box. If you are planning to share personal data with another body and the data subject has consented, check that the body is fully aware of its Data Protection responsibilities. We should make it a condition of sharing the data that the recipient does not share it again, without receiving further 'opt in' consent from the data subjects. Note also the need for secure transmission of the data.

**Whose responsibility is it to ensure that shared data is accurate?**

It is not possible for us to carry out regular checks to ensure the accuracy of all the personal data which we process. However, we must ensure that data subjects are aware of their right to check the accuracy of data held, and their right to amend it.

**How does the Freedom of Information Act affect Data Protection?**

The Freedom of Information Act extended the Data Protection Act to personal information not previously subject to the Act. Any information about an identifiable living individual is now subject to the Act to a greater or lesser extent.

**Can personal data be put on TNA's website?**

In some circumstances, yes. Seek advice on individual circumstances from the Data Protection Officer.

## ANNEX 3 PERSONAL DATA REPORT FORM

Complete this form when you start a new collection or set of personal information, whether held electronically or manually in any other medium, e.g. index cards, paper files, microfiche etc. Exclude word processed documents and Outlook contacts lists.

1 Department responsible for the data	2 Person responsible for the data (name & job title)																
3 Name of collection	4 Description of collection & quantity																
5 Is it held electronically? If so, & networked, specify folder path & file name. If not networked specify Objective folder or pc asset number	6 Is it held manually? If so, & in a registered file series, specify the series. If not in series, give file name																
<p>7 What personal details are included? (tick all that apply)</p> <table border="0"> <tr> <td>Name?</td> <td>Postal address?</td> <td>Phone no?</td> <td>Email address?</td> </tr> <tr> <td>Date of birth?</td> <td>Nationality?</td> <td>Bank details?</td> <td>Religion?</td> </tr> <tr> <td>Research topic?</td> <td>Health details?</td> <td>Disability details?</td> <td></td> </tr> <tr> <td>Trade Union membership?</td> <td></td> <td>Other? (please specify)</td> <td></td> </tr> </table>		Name?	Postal address?	Phone no?	Email address?	Date of birth?	Nationality?	Bank details?	Religion?	Research topic?	Health details?	Disability details?		Trade Union membership?		Other? (please specify)	
Name?	Postal address?	Phone no?	Email address?														
Date of birth?	Nationality?	Bank details?	Religion?														
Research topic?	Health details?	Disability details?															
Trade Union membership?		Other? (please specify)															
<p>8 Who provided the information? (tick all that apply)</p> <table border="0"> <tr> <td>Data subject?</td> <td>TNA staff?</td> <td>Other people? (please specify)</td> </tr> </table>		Data subject?	TNA staff?	Other people? (please specify)													
Data subject?	TNA staff?	Other people? (please specify)															
9 What is the information used for?	10 What has the data subject been told about its use?																

11	Do you disclose the information internally? If so, to whom, why, and what do they use it for?
12	Do you disclose the information externally? If so, to whom, why, and what do they use it for? Does it go outside the UK?

13	When does the information date from?
----	--------------------------------------

14	Is the system new since 24/10/1998?
----	-------------------------------------

15	How long is the information kept?
----	-----------------------------------

16	Is it on a disposal schedule? If so, What is the disposal action?
----	---

17	Who is responsible for carrying out disposal action?
----	--

18	Is destruction recorded?
----	--------------------------

19	What are the security arrangements? <span style="float: right;">(give details for whichever applies)</span> For manual files  For electronic files  For computer output  For information no longer required
----	--

20	Other relevant information
----	----------------------------

Name  
Department

Date

## ANNEX 4 DATA SUBJECT ACCESS REQUEST FORM

### 1 Details of the person requesting the information

Full name

Address

Tel. No.

Fax No

Email address:

### 2 Are you the data subject?

**YES:** If you are the data subject please supply evidence of your identity, i.e. something bearing your signature such as an original or copy driving licence or passport. Originals should be sent by recorded delivery and will be returned to you. **(Please go to question 5)**

**NO:** Are you acting on behalf of the data subject with their written authority? If so, that authority must be sent to us. **(Please complete questions 3 and 4)**

### 3 Details of the data subject (if different from 1)

Full name

Address

Tel. No.

Fax No

Email address:

### 4 Please describe your relationship with the data subject that leads you to make this request for information on their behalf

**5 Please describe the information you seek together with any other relevant information. This will help to identify the information you require.**

**We are allowed charge a fee of £10 for each application. An invoice is enclosed.**

**DECLARATION. To be completed by all applicants. Please note that any attempt to mislead may result in prosecution**

1 ..... certify that the information given on this application form to The National Archives is true. I understand that it is necessary for The National Archives to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data

Signature:

Date:

**Note.** The period of 40 days in which The National Archives must respond to the request will not begin until it is satisfied on these matters.

Please return the completed form to ARK Enquiry Service, The National Archives, Kew, Richmond, Surrey TW9 4DU.

Documents which must accompany this application:

- evidence of your identity
- evidence of the data subject's identity (if different from above)
- authorisation from the data subject to act on their behalf (if applicable)
- the fee set out on the attached invoice
- stamped addressed envelope for return of proof of identity/authority documents

## **ANNEX 5 SUBJECT ACCESS REQUESTS – PERSONAL INFORMATION ABOUT STAFF (PAST AND PRESENT)**

*This annex sets out how subject access requests for current and former members of staff are handled. It is aimed both at staff intending to make such requests (data subjects) and colleagues responding to those requests.*

### **1 Types of personal information held about staff**

This section sets out the types of personal information held about staff so that those intending to submit subject access requests can be specific in their requests, identifying precisely what they seek. The following types of information are held:

- Manual files
  - A file for each member of staff kept by HR, containing for example application form, contract of employment and subsequent changes to terms and conditions letters, sickness certificates, performance management forms.
  - A file for each member of staff kept by the Welfare Officer containing information such as Pre-Employment Health Declarations and information from Occupational Health
  - Files held by line managers containing copies of papers sent to/held by HR (OPSI)
  - Recruitment campaign files containing full documentation of recruitment for one year, then sifted down to basic data which is kept for eighteen months (mostly but not always on electronic files )
- Systems maintained by HR
  - PROMISE/Compel – information system kept by HR, containing summary information including home address, date of birth, job history, absence, training and development details, recruitment campaign records (full data held for one year; basic data held for three years),
  - EPAYFACT – pay system run by Logica cmg (TNA's payroll provider) accessible by HR, containing pay data from 1 April 2003
  - Atracs – records of swipes on the flexi system. Individual electronic records kept for two months, paper records kept for 12 months (from March 2007 replaced by all electronic records)
- Systems maintained by ICTD
  - Websense – log of websites accessed by members of staff. Logs are deleted after 3 months
  - Telephony system – holds details of telephone calls made and received (including date, time, number dialled and duration of call) on all telephones connected to the system, fixed and mobile. Reports can be run by ICTD. Logs are deleted after 3 months

- Mailsweeper – log of incoming and outgoing emails, deleted after 90 days - and MessageLabs, another log of emails, maintained externally and deleted after 1 month.
- Outlook – email, schedules and contacts. Emails are deleted automatically after 3 months
- Information maintained by Security
  - CCTV (Kew only) – Security maintains two CCTV systems. Information held on the analogue CCTV system, which monitors the document reading rooms and invigilation room, is deleted every calendar month. Information held on the digital system, which monitors other areas including the grounds, museum and entrance to Kew 2, is automatically deleted on a rolling basis after 30 days.
  - Access control system – information system kept by Security which records the number of the proximity pass, the pass holder's name, the controlled area the pass was used to access and when. The information is currently held from 2003 but in future will be deleted after 12 months.
- Objective – material within the following functions:
  - Personnel Management – under Performance Management, Attendance Management (sickness, leave and flex adjustments), Establishment (some heads of department have an issues file), and Work Experience. Note that grievance and disciplinary material is filed in Objective temporarily, being deleted when action has been completed, at which point the manual file becomes the source.
  - Recruitment – details retained for eighteen months except fixed term appointments which are kept for the duration of the appointment.
  - Staff development – e.g. training course evaluation summaries, Further Education funding applications, training logs
  - Incidental references may occur elsewhere, e.g. within minutes of meetings
  - Home (personal) folder – e.g. of managers
  - PSI holds equivalent information on shared drives
- DORIS – information system with reader ticket details and details of records consulted. For the purposes of subject access requests this is regarded as being kept by Document Services. Data held electronically dates back to May 1999

## **2 Making a subject access request**

Requests for access to any of this personal information should be sent to HR, clearly identified as subject access requests. Requests must be in writing and can be by email. Emails should be sent to the HR mailbox.

If members of staff are interested in particular information e.g. information about them held in a specific system listed above or relating to a specific

matter, they should describe the information sought in their request. The more specific the request, the more effective the response will be.

If they want someone else to view the information on their behalf, or to accompany them when they view the information about them, they should make this clear in their request for access. The authorisation (which can be by email) must be for a named person, i.e. 'a union rep' will not be sufficient, the name of the individual must be given.

HR will not normally apply the standard £10 fee to requests from current members of staff but reserves the right to apply it to requests from former members of staff.

### **3 Receipt, logging and analysis of requests**

All requests for access will be handled by the Human Resources Operations Manager in the first instance, or the HR Information Systems Officer in her absence. She will analyse the request to see whether any systems held outside HR are covered and, if so, will contact the relevant people and co-ordinate the response. If the request is solely for CCTV it will be passed to the Head of Security to deal with.

All requests will be logged and tracked on the FOI Tracking System, Supportworks.

### **4 Retrieval and assessment of information**

It is possible that some requested information will not be provided because it is subject to one or more of the exemptions in the Data Protection Act. Information may be exempt, for example because it relates to a third party (i.e. another data subject) whose interests need protecting. The HR officer handling the request will examine the file to see whether exemptions apply and will redact as necessary so as to enable the rest of the information to be provided.

For information within Objective, the records manager will provide the Human Resources Operations Manager with a report listing items in Objective where the individual is named. The report can be configured to focus on certain files, dates or individuals, and may include the contents of Home Folders. HR will assess whether any of the contents of this report might be subject to one of the exemptions in the Data Protection Act and redact as necessary.

CCTV will be examined to see whether third parties are visible and, if so, whether release of the images would be likely to cause damage or distress to those third parties. If so, redaction will be undertaken.

### **5 Provision of access to information**

HR will arrange an appointment with the individual to view his/her personal and welfare files. These files may only be viewed within HR (with the

exception of staff based in Norwich) and under the supervision of a member of the Department. Information that is held electronically will be forwarded to the individual by email.

If the data subject has nominated someone else to view the information on their behalf, an appointment will be made with that person. If the person is not known to HR, their pass will be checked to verify that they are who they say they are. This is to protect the privacy of the data subject.

For Saturday workers this appointment can be either on the Saturday morning each month on which HR staff are present at Kew or on another day.

At this appointment the individual will be supplied with printouts or copies of information from other systems that fall within the scope of the request. For information in Objective, HR will provide the report mentioned at section 4 above. If the data subject wishes to access specific items listed in the report but is unable to do so due to access privileges in Objective, the Human Resources Operations Manager will arrange access.

HR will provide photocopies of documents on the manual files on request.

CCTV will be provided on a disc.

## **6 Timescales**

The statutory period for dealing with requests is 40 days; however wherever possible HR will make the manual files and information from its information systems available within 10 working days of receipt of any request. All other information will be provided within 40 days. If you can demonstrate an urgent need requiring a quicker response, HR will treat this sympathetically whenever possible.

For Saturday only workers and staff based in Norwich, it may not be possible to provide access within 10 working days.

## **ANNEX 6 EXEMPTIONS FROM DATA SUBJECT ACCESS RIGHTS**

1 FOI exemptions and EIR exceptions do not apply when data subjects ask for information about themselves and the request is being handled under the Data Protection Act.

2 The main grounds for refusing to provide information in response to a subject access request are:

- To safeguard national security (DPA section 28). A Ministerial Certificate can be issued to that effect but can be appealed to the Information Tribunal
- To avoid prejudicing the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty (DPA section 29)
- An Order has been laid exempting subject access to health information, educational records or social work records where this would have an adverse effect on the data subject (DPA section 30)
- To avoid prejudicing regulatory activity by specified bodies (DPA section 31)
- Processing is for journalistic or literary purposes with a view to publication (DPA section 32)
- Processing is for historical or other research and is subject to specified conditions (DPA section 33)
- Information is available already under another Act
- Confidential references provided (not received) by TNA

3 If there is any possibility any of these exemptions might apply, consult the Data Protection Officer.