PROCEDURES FOR HANDLING PERSONAL INFORMATION UNDER THE

DATA PROTECTION ACT 1998

[*These procedures are in the process of being updated in order to comply with the forthcoming Data Protection Act and the European Union General Data Protection Regulations (GDPR)]*

Contents list

1 Scope of the procedures

2 Roles and responsibilities

3 Acquiring/creating and using personal data

4 Keeping personal data accurate

5 Retaining or destroying personal data

6 Keeping personal data secure

7 Subject access requests

8 Sharing personal data with 3rd parties

9 Sending personal data out of the country

10 Personal data in the archives

11 Further information and advice

Annex 1 Definitions of data protection terms

Annex 2 Data Protection Principles

Annex 3 Frequently asked questions

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 on 16 November 2011 – updated with new Data Protection Officer contact details in April 2013)

1 SCOPE OF THE PROCEDURES

1.1 These procedures complement the Data Protection Policy Statement. Both the policy and procedures are published on our website here http://www.nationalarchives.gov.uk/legal/information-charter.htm .

1.2 The procedures apply to all personal data created or collected by TNA staff in the course of their daily work. This includes:

- information held by managers about their staff, such as absence and performance management details
- the names and other details of people who hold readers' tickets, attend events here or serve on our advisory or consultative groups
- the names and other details of people who contact us by letter, email, fax or telephone
- mailing lists of all kinds
- the names and details of staff in government departments and other public bodies
- information about contractors and suppliers of goods and services
- emails, where either the person sending or receiving is identifiable or the contents refer to identifiable people
- word processed documents, spreadsheets and databases which contain personal details such as names and addresses

1.3 Personal data is generally held in systems such as the CRM (Customer Relationship Management database), DORIS (reader information), MyHR (the main HR system,), Objective (our records management system) etc but can be found also in individual mailboxes and contacts lists in Outlook. They include systems managed on TNA's behalf by third parties.

1.4 **The general rule is 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.**

1.5 The procedures apply also to some of our archival holdings – see section 10 for details.

1.6 See Annex 1 for explanations of some terms used in these procedures. See Annex 2 for the Data Protection Principles referred to in these procedures.

2 ROLES AND RESPONSIBILITIES

The Data Protection Officer (Linda Stewart) has operational responsibility for data protection within The National Archives. She advises on what is necessary for compliance, liaises with the Information Commissioner's Office (ICO) which regulates data protection, liaises with staff in other government departments on data protection policy development, and deals with some information requests.
2.2 She is assisted by two deputies who provide support and cover in her absence, as follows:
Mark Hanvey (MH) – Data Protection Principle 7 (data security) matters

Michael Appleby (MA) - other data protection principal matters; including responsibility for dealing with subject access requests and matters that affect information management..

2.3 Others also have a role and responsibilities:
The Operations Director Paul Davies is accountable to Management Board and the Executive Team for data protection in his capacity as Chair of the Departmental Security Committee and Senior Information Risk Owner for The National Archives

The Head of Knowledge and Information Management (Simon Lovett) - ensures that personal data within our corporate records and information systems is managed in compliance with the Data Protection Principles.

The Departmental Security Officer (Chris Cooper) - as Accreditor of The National Archives‟ information systems, ensures that these systems and their operating procedures comply with the personal data and other requirements of HMG‟s *Security Policy Framework.*

Information Asset Owners – IAOs are appointed at head of department level and are responsible for managing the risks, including data protection risks, to the information that is produced, received, owned and managed by their business area. This information can sit across a number of systems. Each IAO must certify twice yearly to the SIRO that information risks in their area have been identified and are being managed.

Information Asset Managers – IAMs (formerly Departmental Records Managers) are responsible for maintaining the file plan in Objective and for keeping the departmental „what to keep‟ schedule current. They support their departmental IAO.

Managers – ensure all their staff attend data protection training and are aware of their responsibiities concerning personal data.

All staff - all members of staff, including temporary staff, have personal responsibility for following these procedures. They should be followed also by contractors using The National Archives‟ systems.

3 ACQUIRING/CREATING AND USING PERSONAL DATA

This section sets out good practice to be followed when creating or acquiring and using personal data.

3.1 The Data Protection Act is about collecting and using personal data in a way that is lawful, fair to the individuals the information is about (the data subjects) and meets their reasonable expectations. There are some specific provisions, e.g. to expand upon what fairness involves, but essentially that is what it is about.

3.2 Here are some good practice **DOs** and **DON'Ts** for collecting or acquiring and using personal data. They are under these headings:

- Think ahead
- Justify your collection and use of personal data
- Be transparent about your intentions
- Get consent from data subjects
- Collect and use as little personal data as possible

Think ahead

3.3 The **DOs** and **DON'Ts** in this section require you to have given some thought to what you are trying to achieve and how best to do it, e.g. you cannot be open and honest about your intentions if you have not decided why you need the personal data and how you plan to use it, now and in the future.

DO think about what you are planning to do before you do it.

DO consult the Data Protection Officer about whether you need to do a Privacy Impact Assessment before you start.

DO consult the Accreditor at an early stage if you are creating a new system or significantly changing an existing system, since it will need to be accredited. The Accreditor will ensure that the system's technical capabilities and operational procedures meet data protection (and other) requirements.

DON'T ignore data protection considerations at the early stages thinking that you can cover them later.

Justify your collection and use of personal data

3.4 Our collection and use of personal data must always be

- fair to the person the information is about
- lawful, i.e. not forbidden by law, and
- necessary in terms of the one of the justifications set out in the Act

The following **DO's** and **DON'Ts** deal with each of these aspects.

Fairness

3.5 Fairness is about acting within the expectations of the person concerned.

DO think about what they would expect you to do and not do with 'their' personal data and act accordingly. If you are uncertain, **DO** put yourself in their position and ask yourself what you would like and expect to happen.

DO keep the promises we make in the Privacy Notice (see below). **DO** use personal data only for the purpose(s) for which it was obtained or for compatible, i.e. reasonably similar, purposes. For example, **DON'T** use information collected for research purposes for marketing purposes unless the individual has consented to this different use.

DON'T make negative comments about individuals unless they are based on recorded facts and can be defended as accurate if challenged. Whenever you write anything about individuals, **DO** remember that quite apart from the importance of fairness, people have a right to ask to see what you have written about them.

Lawfulness

3.6 Lawfulness is about ensuring you keep within the law, e.g. **DON'T** write defamatory or obscene comments or disclose personal data in breach of other legislation.

The justification

3.7 The best justification is the consent of the individual (see below).

3.8 If you do not have consent but you need to do what you are doing in order to make progress on meeting an objective or target in TNA's current corporate and business plan, then it is possible – but not certain – that you can go ahead without breaching the Act, but **DO** check with the Data Protection Officer first.

3.9 If you do not have consent or cannot make this link to our corporate and business plan but really need to use the personal information, **DO** consult the Data Protection Officer.

3.10 if you are using sensitive personal data (information about people's health, sex life, religion etc – see Annex 1) **DO** be particularly careful. As well

as being fair to the person the information is about, and lawful, **DO** make sure that what you plan to do is necessary in terms of one of these justifications:

- we have consent
- we need to do it to meet a corporate objective
- we need to do it for employment purposes
- the information has already been made public by the person concerned
- we need to do it in connection with legal proceedings, to obtain legal advice or to establish or defend legal rights
- we need to do it for ethnic monitoring purposes
- we need to do it to protect the vital interests of the data subject or another person and obtaining consent is not an option
- we are doing it for research purposes and we will neither make decisions affecting the individual nor cause them substantial damage or distress

3.11 **DO** consult the Data Protection Officer before taking action. **DON'T** take any risks.

Be transparent about your intentions

3.12 We are required to be open and honest with people about how we propose to use 'their' personal data. We do this by giving them a Privacy Notice at the time we obtain it. Here are some of the points we might need to cover:

Why we need their personal data

3.13 Unless it is already obvious from the context, **DO** tell people why we need their personal details. For example, if someone orders a book from the bookshop, we need their name and address to post it to them. In this case the reason we need their postal address is so obvious that we do not need to tell them.

3.14 In other cases it might be less obvious. For example, people applying for a reader ticket might not realise why we need all the personal details we request so **DO** give them an explanation.

What else we might do with their personal data

3.15 People who order a book from the bookshop or make a telephone enquiry would not necessarily expect further contact from us. If we want to do

anything they might not expect, e.g. add them to our CRM or send them our enewsletter, **DO** seek their consent (see 4 below).

Whether we wish to share their personal data with another body, e.g. another government department

3.16 There may be a statutory basis for sharing their personal data with others – **DO** ask the Data Protection Officer whether this is the case. If not, **DO** give the person a chance to give or refuse consent to sharing their information with others, e.g. another archives institution or government department. **DON'T** assume they will not object.

Whether we wish to export the personal data

3.17 This is an issue if we want to send the information outside the European Economic Area (the European Union countries plus Norway, Liechtenstein and Iceland). (See section 9.) **DO** consult the Data Protection Officer.

Privacy notices

3.18 The Privacy Notice must be in Plain English, in reasonably prominent type, and in a reasonably prominent position on the form or screen. **DO** make sure it is clear who we are and give our name in full, i.e. The National Archives.

3.19 The Privacy Notice need not be complicated – it depends on what we intend to do with their personal data and how obvious that will be to the person. **DO** use a simple sentence such as this if possible:

> *We will use your personal details only to process your order*

together with a reference to our Privacy Policy on our website.

3.20 If necessary, **DO** provide more detail, e.g.

> *When you sign up to our mailing list the information that you provide will be used to send you our monthly enewsletter and other information that we have not included in the enewsletter but think may be of interest to you. We use an email distribution company to send out our e-marketing communications but your data will not be passed on to any other third parties. You can remove your details from our database at any time by following the link at the bottom of every email that we send you. For more information read our privacy policy.*

3.21 If you want consent to share personal data with interested parties **DO** include a sentence like this:

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

3.22 **DO** consult the Data Protection Officer about new Privacy Notices before finalising them.

Telephone calls

3.23 If you are doing business by telephone **DO** include an equivalent form of words in the conversation. This is particularly important if you intend to do anything more than deliver what they have asked for during the telephone conversation, e.g. add them to our CRM or the mailing list for our enewsletter.

Get consent from data subjects

3.24 If we have any plans to keep and use people's personal data for some other purpose, and they would not expect us to use it for that purpose, we must seek their consent.

DON'T assume people will be willing for us to use 'their' personal data in a different way just because it seems obvious or sensible to us. **DO** put yourself in their place and consider their expectations.

DO ask people to opt-in to different use of their personal data rather than to opt-out from it. If you want to ask data subjects to opt-out rather than opt-in, **DO** consult the Data Protection Officer first.

If you are dealing with sensitive personal data (see Annex 1) **DO** always include an opt-in rather than an opt-out box on the form or screen.

With sensitive personal data, consent must be active. **DON'T** assume someone has consented just because they have not responded with an explicit refusal.

DO keep the evidence of consent for as long as you keep the personal data.

On a web form **DO** put something like this:

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 for this purpose <box>

To get consent during a telephone call **DO** say something like this:

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.

Collect and use as little personal data as possible

3.25 The 3rd data protection principle says that personal data must be 'adequate, relevant and not excessive'. This means collecting and using the minimum of personal data required for the particular purpose, i.e. enough but not too much.

DO collect only the personal data you really need to achieve your objective.

DON'T collect irrelevant information simply because it might be useful at some point in the future – you need to be able to explain why each type of personal data is necessary.

DO think also about whether depersonalised or anonymous information would achieve the same result as information with a name attached, e.g. a feedback form or survey questionnaire needs the name of the person completing it only if you intend to follow it up with the person.

Keep personal data in an accredited system

3.26 **DO** store any personal data acquired in the course of work in an accredited system. Accredited systems are those formally recognised by The National Archives as having the functionality and management arrangements required for management of the risk they present. Outlook and Objective are both accredited systems.

3.27 If you are planning to start a new system or significantly change an existing one, **DO** remember that it is likely to need a Privacy Impact Assessment, a Security Risk Assessment and accreditation by the Accreditor (see section 2 above for a description of his role). Guidance on these are available from the Data Protection Officer, the Deputy Data Protection Officer (MH) and the Departmental Security Officer respectively.

3.28 **DON'T** forget that paper files are also considered a system and are therefore subject to the same risk assessment and other procedures as electronic files. If you are thinking about developing a new system to hold personal data, **DO** consult the KIM Team, ICT and, for major projects, Strategic Projects.

4 KEEPING PERSONAL DATA ACCURATE

This section explains the need to keep personal data accurate and up to date and what you should do about correcting inaccurate personal data. It does not apply to personal data in the archives.

4.1 Any personal data that we keep and use should be accurate and up-to-date. We are not expected to achieve total accuracy but should take

'reasonable' steps to ensure accuracy, e.g. by making sure to update addresses when notified of changes.

4.2 Here are some good practice **DOs** and **DON'Ts** for keeping personal data accurate and up to date. They are under the following headings:

- Check accuracy at the point of collection
- Correct personal data on request
- Pass on corrections to personal data internally
- Pass on corrections to personal data externally

Check accuracy at the point of collection

4.3 It is reasonable to assume that people providing 'their' personal data directly will do so accurately. However …

If you are transcribing personal data provided over the telephone, or from one form to another, **DO** take care to do so accurately and **DO** double-check with the individual if in any doubt.

If you receive personal data about an individual from a third party, **DO** check how accurate the person providing the information believes it to be and, if there is doubt about accuracy, **DO** keep a record of this in case you have to reply to a subsequent complaint from the data subject.

Correct personal data on request

4.4 People have the right under section 14 of the Data Protection Act to ask for correction of their personal data.

If someone states that information about them is inaccurate and can provide evidence to support this, **DO** make the correction – **unless** the personal data is in the archives, in which case **DON'T** make the correction but instead **DO** refer the request to the Data Protection Officer. (See section 10 of these procedures for further guidance.)

DO consider whether you need to keep a record of the correction. This will depend on the nature of the information. For example, it is rarely necessary to record a simple change of address. With something more complex that could affect the rights of the person concerned, or that you might need to refer to later, **DO** keep a record of having made the correction.

DO consider also whether you need to retain the incorrect data previously used for decision-making. If you do, and the system does not retain previous versions of data automatically, **DO** keep the content as it was before correction and file it with a record of the correction.

4.4 If you have any doubts or concerns, **DO** consult the Data Protection Officer.

Pass on corrections to personal data internally

4.5 If you are correcting personal data **DO** consider whether it might have been passed to another part of The National Archives and, if so, whether colleagues should be informed of the correction. For example, if readers change their addresses for reader ticket purposes, **DO** check the CRM to see whether updating is needed. Similarly, if Marketing and Communications is notified that someone on a mailing list has died, **DO** tell Document Services so that DORIS can be updated and the reader ticket cancelled.

Pass on corrections to personal data externally

4.6 It is possible the personal data was disclosed to a third party some years ago for a specific purpose, for example in connection with a job application. Sending a note of the correction is unlikely to be necessary. If in doubt, **DO** consult the Data Protection Officer.

5 RETAINING OR DESTROYING PERSONAL DATA

This section sets out the need to make decisions about keeping or destroying personal data and to implement those decisions. It does not apply to personal data in the archives.

5.1 The Data Protection Act says that personal data should not be kept for longer than necessary. Just how long that should be is left to The National Archives to decide but we may have to defend our retention practices to the Information Commissioner.

5.2 Here are some good practice **DOs** and **DON'Ts** about retention/disposal. They are under the following headings:

- Think corporately
- Take personal responsibility
- Destroy securely

Think corporately

5.3 If personal data is being kept for the corporate record, **DO** make sure it is included in your department's What to Keep schedule. Your IAM can advise how to do this.

Take personal responsibility

5.4 Each member of staff is responsible for managing their own Outlook mailbox and their personal space in Objective:

DO file or delete incoming and outgoing emails once the action to which they relate has taken place, if not earlier. At regular intervals **DO** review those which remain in a personal mailbox pending a final decision and either file or delete them. It is particularly important that you **DON'T** keep emails containing sensitive personal data, for example information about someone's health, in your mailbox indefinitely

DO apply the same disciplines to shared mailboxes. **DO** make sure that someone in the team that uses it has lead responsibility for managing a shared mailbox

DO review the contents of personal folders at regular intervals and file anything that should form part of our corporate record in Objective.

Destroy securely

5.5 When deleting personal data held electronically, **DO** ensure that it is removed from the Recycle Bin.

5.6 **DO** destroy paper-based personal data under secure conditions - shred it or use a Confidential Waste bag which should be closed and collected by Facilities on the same day. **DON'T** just put it in the blue recycling bin.

6 KEEPING PERSONAL DATA SECURE

This section gives some basic guidelines about the safekeeping of personal data and its protection from loss, damage or unauthorised access.

6.1 It is very important that personal data 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 large number of people (1000+). Failures elsewhere have led to damaging publicity.

6.2 Here are some good practice **DOs** and **DON'Ts** for data security. They are under the following headings:

- Store personal data securely
- Transmit personal data securely
- Take care with telephone calls
- Report loss, unplanned destruction or damage

Store personal information securely

6.3 **DO** make sure that personal data 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:

DON'T leave paper copies of personal data where anyone else can access them. **DO** keep paper records locked away securely

DO lock your computer before leaving it or even moving away so that you can no longer see it. **DO** this also if you have a visitor who should not see the information on your screen

If you are keeping sensitive personal data in Objective, **DO** set the privileges so that it can be accessed only by those with a need and a right to see it. See separate guidance on Narnia [link to intranet removed].

If the personal data is held outside Objective and is not common knowledge, **DO** use passwords to secure it

6.4 In general, **DO** follow the data handling guidance on Narnia [link to intranet removed].

6.5 If you have any doubts, **DO** consult the Deputy Data Protection Officer (MH).

Transmit personal data securely

6.6 If you are transmitting personal data, whether internally within The National Archives or externally, i.e. to another body, **DO** ensure a level of security appropriate to the nature of the data. For example, if you are sending copies of a closed record to a member of the public in response to a subject access request, **DO** take the precautions described below. (See sections 7 and 10 for more on subject access requests.)

Transmission within the National Archives

6.7 Even moving personal data within The National Archives requires some precautions:

If you are using physical means such as an envelope, **DO** ensure the envelope is sealed and alert the recipient to the fact that you have sent it.

If you are sending personal data between Kew and Norwich, **DO** follow the guidelines for external transmission below.

If you are using email, **DO** ensure the email is protectively marked (the appropriate protective marking will usually be PROTECT – PERSONAL).

Transmission outside The National Archives

6.8 Sending personal data outside The National Archives requires these precautions:

If you are using the post or a courier, **DO** double envelope the personal data and ensure both envelopes are marked for the attention of a named person. **DO** use recorded delivery if sending it by post.

If you are using email, **DO** get IT to encrypt the personal data, ensure the email is protectively marked, and send the password or key for decryption separately

DO ensure the transmission is made using a system approved by the Accreditor for that purposes; if not, **DO** ensure the transmission has been approved by the Director, Technology and **DO** consult the Deputy Data Protection Officer (MH) or one of his colleagues in IT about the method and device to be used. This may include encrypting the personal data, send it by recorded delivery or courier, and sending the password or key for decryption separately.

Take care with telephone calls

6.9 Phone calls can lead to unauthorised use or disclosure of personal data so **DO** take the following precautions:

If you receive a phone call asking for personal details of a colleague to be checked or confirmed, **DON'T** automatically provide them. The phone call may come from someone pretending to be the data subject, or impersonating someone else who would have a right of access. **DO** check identity first and **DON'T** reveal information the colleague might prefer not to be revealed. If you have any doubts, **DO** either ask the enquirer to put their request in writing or take their name and contact details and pass the enquiry to your manager or the Data Protection Officer.

If a phone call seeks personal data about a member of the public, the same issues arise. **DO** either ask the enquirer to put their request in writing or take their name and contact details and pass the enquiry to your manager or the Data Protection Officer.

If you have established that the caller does have a right of access to the personal data but you think the data subject would regard it as private, **DO** ensure that you cannot be overheard when providing it. If colleagues sitting close to you could overhear you **DO** move the phone conversation to a room where you can have privacy

DO check the identity of the enquirer (see section 7 below for guidance on this)

DON'T provide a home address, phone number or email address without the person's explicit consent.

Report loss, unplanned destruction or damage

6.10 **DO** keep unauthorised or accidental access, alteration, disclosure, destruction or loss of personal data to a minimum. Sometimes, despite taking precautions, things go wrong. If that happens, **DO** record the circumstances and report the incident as soon as possible to the Departmental Security Officer.

7 SUBJECT ACCESS REQUESTS

This section outlines the access rights of individuals in relation to 'their' personal data and how to respond to requests. It does not apply to personal data in the archives, for which see section 10.

7.1 Data subjects (the individuals the personal data is about) have certain access rights:

- to be told whether personal data about them is held and being used
- to be given a description of the personal data, told how it is being used, and given details of others to whom it is or has been disclosed
- to see the personal data in intelligible form
- to be told how it was obtained

7.2 Requests from data subjects relating to information about themselves are called subject access requests. Sometimes these requests come from people acting on behalf of the data subject, e.g. a family member or a solicitor. If the person making the request is acting on behalf of the data subject it counts as a data subject access request.

7.3 Here are some good practice **DOs** and **DON'Ts**. They are under the following headings:

- Check that subject access requests are valid
- Forward to the FOI Centre for co-ordination
- Check entitlement to the personal data
- Ensure people making requests on behalf of a data subject are genuine
- Fees
- Respond to the request
- Special procedures for staff access to 'their' personal data

Check that subject access requests are valid

7.4 To be valid, subject access requests must be **in writing**, either on a form such as at Annex 4 or in a letter or email. **DO** ask anyone making an oral request to put it in writing and offer a copy of the form at Annex 4.

Forward to the FOI Centre for co-ordination

7.5 Action on subject access requests is co-ordinated by the Deputy Data Protection Officer (YCT) so **DO** forward subject access requests to her in the FOI Centre on receipt. The FOI Centre's mailbox is FOIcentre@nationalarchives.gsi.gov.uk .

Check entitlement to the personal data

7.6 Before we provide the personal data we must be satisfied that the person is entitled to it. How thoroughly you check this entitlement depends on the sensitivity of the personal data requested and whether the individual is known to you already. There are two parts to this check:

- Checking the identify of the person
- Checking the person is the same person as the data subject

Checking the identity of the person

7.7 This is done to make sure he is who he says he is (for example, he is really John Smith). You need to do this if you don't know the person already.

DO check identity using any of the following.

- Passport
- National identity card
- Driving licence (if it has a signature, check it against the enquirer's, if the request was posted)
- UK civil service photo-pass (again with a signature), or a company or university photo-pass (if it identifies the company or university and bears a signature)

If the applicant does not provide one of the above, **DO** check with the Deputy Data Protection Officer (YCT) whether the alternative offered is acceptable.

7.8 We accept copies but prefer to see the originals. **DO** keep a copy on the case file in Objective and **DO** remember to return the originals to the enquirer using recorded delivery.

Checking the person is the same person as the data subject

7.9 This is done to ensure we do not disclose personal data to the wrong person. You need to do this if you are not already certain e.g. because he or she is a colleague.

7.10 To check that he is the same John Smith as the one we hold personal data about, **DO** draw on the personal data to ask questions which an impersonator should not be able to answer.

Ensure people making requests on behalf of a data subject are genuine

7.11 Here are some simple precautions to take:

DON'T provide personal data to someone claiming to act on behalf of the data subject unless they have written authorisation signed by the data subject and evidence that it is genuine (for example, proof of their relationship to the data subject, such as a full birth certificate).

DO carry out the entitlement checks described above also.

Fees

7.12 There is a statutory fee of £10 for responding to subject access requests which can be waived if we choose. This does not recover our costs and we often waive it. **DO** consult the Deputy Data Protection Officer (YCT) if you think the fee should be levied.

Respond to the request

Deadline for response

7.13 Under the Data Protection Act, the deadline for responding to subject access requests is 40 calendar days. **DO** make sure to meet this deadline.

Using standard paragraphs in replies

7.14 **DO** use standard paragraphs when putting together the response to accompany the requested personal data. It is important in particular to make it clear that the request has been handled under the Data Protection Act and to explain rights of redress. The standard paragraphs can be found in Objective here [link to document in Objective removed].

Providing the requested personal data

7.15 As far as possible **DO** meet the applicant's requirements with regard to format and method of despatch, although you need not digitise personal data held manually. **DO** label what you are sending so that the applicant can make sense of it.

Special procedures for staff access to 'their' personal data

7.16 Special arrangements apply to requests by staff for personal data held about them, including their personnel records in HR - see Annex 5.

7.17 If in doubt at any point, **DO** consult the Deputy Data Protection Officer (YCT).

8 SHARING PERSONAL DATA WITH THIRD PARTIES

This section explains how to handle requests for personal data from 3rd parties who are not acting on behalf of the data subject, and also other proposals to share personal data with 3rd parties. It does not apply to personal data in the archives, for which see section 10.

8.1 The Data Protection Act does not give third parties a right of access to personal data although it does not absolutely prohibit such access.

8.2 Here are some good practice **DOs** and **DON'Ts** for the five main categories of sharing with 3rd parties. These categories are as follows:

- Requests from the police or other investigative bodies
- Requests from government departments for details of who has seen records transferred by them
- Requests from members of the public or businesses
- Personal data intended for statistical or other research use
- Personal data shared to obtain a service

Requests from the police and other investigative bodies

8.3 The Data Protection Act allows us to release personal data to the Police and other investigative bodies in connection with preventing or detecting crime and catching and prosecuting suspects. ACPO (the Association of Chief Poice Officers) has developed a protocol and form which should be used.

DO ask anyone making an oral request to put it in writing and suggest they use the template developed by ACPO.

DO forward all such requests to the Data Protection Officer who will assess them, decide whether the request provides sufficient justification for disclosure of personal data and, if so, co-ordinate the searches required. If any information is found, the Data Protection Officer will arrange for it to be provided and will keep a record of the event so that there is a clear audit trail.

The police may make requests for access to closed records as part of an ongoing investigation. **DO** refer these requests to the Deputy Data Protection Officer (YCT) for advice. (The preferred course of action might be for the request to be made to the transferring department which would retrieve the records to deal with the request.)

Requests from government departments for details of who has seen records transferred by them

8.4 As a general rule we don't supply a department with the names or any other details of members of the public who have looked at records transferred by that department. In exceptional circumstances we will do so if authorised by the Director, Technology or, in his absence, the Data Protection Officer.

DO forward requests from departments – which must be in writing – to the Data Protection Officer in the first instance. She will assess the request and consult the Director, Technology.

If handling such a request, **DO** keep a record so that there is a clear audit trail

Requests from members of the public or businesses

8.5 As a general rule, **DON'T** do any of the following:

- Share the personal data of a member of the public with 3rd parties without their consent. The exceptions to this general rule are the circumstances at 1 and 2 above, which would override the need for consent, and when you are referring people to experts in a particular field who publicise that expertise.

- Provide contact details of other business contacts, e.g. in other government departments, without their consent

- Provide contact details of colleagues who don't have a public facing role. Instead, **DO** take the enquirer's contact details and pass them to your colleague to follow-up. (If the colleague has a public facing role which involves their name being made known, **DO** supply the information unless there is a particular reason not to.)

8.6 If there are special circumstances, e.g. you are aware that your colleague does not want their place of employment to be known, **DO** be careful not to confirm the fact that they work at The National Archives during the conversation. Instead, **DO** take the enquirer's contact details, say that you do not know whether the individual works here or not but will investigate, and pass the enquiry to your manager.

8.7 **DO** assess all requests carefully, whether oral or in writing, to determine whether the interest of the data subject or the office are at stake. **DO** be aware that providing personal details can lead to social engineering attacks, such as phone hoaxes or impersonation using the details you have

provided, which can give outsiders access to our systems and undermine our data security.

8.8 If you have any doubts about providing the personal data, **DO** ask the enquirer to put their request in writing and forward it to the FOI Centre to be handled as an FOI request.

Personal data intended for statistical or other research use

8.9 We are occasionally asked for sets of personal data for use in a research project, e.g. we have been asked for details of FOI requests received by TNA. Caution is needed.

DON'T provide data without first anonymising it so that individuals cannot be identified. It is most unlikely that our Privacy Notice will have included such research use and, without data subject consent to this further use, we could be in breach of the Data Protection Act if we provide data in which people can be identified.

If anonymisation before supplying the data is not possible for some reason, **DO** seek approval to proceed from the Director, Technology and the Data Protection Officer.

DO ensure that if any personal data is being supplied, it is the minimum necessary for the research to proceed.

DO ensure that if any personal data is being supplied, it is transmitted securely in accordance with section 6 of these procedures.

DO ensure that if any personal data is being supplied, there is a written agreement covering the way it will be handled and the precautions that will be taken to protect the interests of data subjects. **DO** consult the Data Protection Officer about the terms of such a draft agreement.

Personal data shared to obtain a service

8.10 We occasionally share personal data in order to obtain a service. Examples are employment data provided to Logica for payroll management purposes, and the email addresses of subscribers provided to the company that distributes our newsletters.

DON'T share personal data unless there is a contract that contains approved clauses regarding data protection compliance.

DO share the minimum of personal data that is required to provide the service.

DO ensure that the Privacy Notice provided to data subjects when the personal data was obtained gives 'cover' for the proposed data sharing.

DO consult the Data Protection Officer about all proposals to share personal data in this way.

9 SENDING PERSONAL DATA OUT OF THE COUNTRY

This section provides alerts to problems with exporting personal data.

9.1 The Data Protection Act limits the transfer of personal data outside the European Economic Area (European Union countries plus Norway, Liechtenstein and Iceland). Transfer means physically transporting the data overseas as well as providing people abroad with access to the information, for example, via the internet.

9.2 Here are some good practice **DOs** and **DON'Ts**.

Except in response to a request from the data subject (the person the information relates to), **DON'T** transfer personal information about living individuals outside the European Economic Area (EU countries, Iceland, Liechtenstein and Norway) unless:

- the data subject has given consent
- a contract is in place which provides equivalent protection of people's rights
- the destination is a country approved by the Information Commissioner for export purposes – see http://www.informationcommissioner.gov.uk/eventual.aspx?id=1163 or
- an exemption from the limitations in the Data Protection Act applies
- the Data Protection Officer has given the go-ahead

DON'T place on our website personal information about staff, other than names, email addresses and, in some circumstances, work responsibilities, without their consent.

DON'T add descriptions to the Catalogue if they contain personal data about identifiable living individuals that could cause them substantial damage or distress, endanger them, or amount to a breach of their privacy.

DON'T place archives on our website that contain personal information about identifiable living individuals without first consulting the Data Protection Officer.

DON'T send copies of closed records to addresses outside the European Economic Area without first consulting the Data Protection Officer. If copies are to be sent, **DO** include with the copies a warning that the recipient should respect the privacy rights of any 3rd parties appearing in the records.

10 PERSONAL DATA IN THE ARCHIVES

This section deals with special provisions applying to personal data in the archives, including subject access requests, requests for correction to data and complaints about our use of personal data.

10.1 The Data Protection Act applies to all archives containing personal information about identifiable living individuals, but there are some exemptions from its provisions for personal information in archives that are kept here for historical research purposes. The key rights to be respected are:

- The right of access to 'their' personal data - subject access requests
- The right to seek correction or destruction of 'their' data
- The right to complain about our use of 'their' data

10.2 Here are some good practice **DOs** and **DON'Ts** for each of these rights.

Subject access requests

10.3 Under section 7 of the Data Protection Act, people can ask us for any personal data relating to themselves that is within the archives. These are called subject access requests. The thing that distinguishes subject access requests from FOI requests is that the applicant is asking for information relating to himself.

10.4 Occasionally the request comes from someone acting on behalf of the data subject, such as a solicitor. If that person has been authorised to act on behalf of the data subject it is still a subject access request but one made through an agent. It is only an FOI request if the request comes from a third party who is not acting on behalf of the data subject.

10.5 There are different provisions for **open** and **closed** records.

Open records

10.6 There is no exemption for open records and we must search for and provide the personal data requested. There is a fixed fee of £10 that we usually charge.

10.7 The only limitation on our obligation to find and provide the personal data is if the data subject has not provided sufficient details in the request for us to be able to identify and locate it. If they have not:

DO acknowledge their request and ask them to supply further details

DO be as specific as possible about what details we need, e.g. their date of birth and country of origin for naturalisation records

If the request does not specify a particular category of records, **DO** ask a question to narrow the search, e.g. which government body they worked for and the date range, or what dealings they had with a government body that makes them believe we might hold their personal data.

DO use the suggested form of words in Objective [link to document in Objective removed].

10.8 If they cannot or will not not supply further details, we are not obliged to comply with the request – we do not have to undertake speculative searches.

DO consult your manager or the Deputy Data Protection Officer (YCT) about whether to refuse the request on these grounds

If you are refusing, **DO** use the standard paragraphs in Objective [link to document in Objective removed] in your letter/email of refusal

10.9 If it is clear from the details provided by the data subject that the personal data is within unstructured manual records (category (e) personal data, explained in ANNEX 1) and undertaking a search would exceed the FOI cost limit of £600 (24 hours work), we can refuse to handle the request.

DO consult your manager about whether to do so

If you decide to refuse to handle the request, **DO** use the standard paragraphs in Objective [link to document in Objective removed] in your letter/email of refusal

10.10 Once it is clear what the applicant wants, **DO** the usual searches of the Catalogue or specialised indexes to find the requested information.

10.11 Special arrangements are in place for some categories of records, e.g. naturalisation indexes, merchant navy service records, change of name records, so **DO** follow them.

10.12 **DON'T** bother to check entitlement unless you think the applicant is not, in fact, the data subject and hence FOI search fees should apply instead of the fixed fee of £10 for subject access requests; there is no other reason to check entitlement if the records are open. (For guidance on checking entitlement see section 7.)

10.13 When providing the personal data, **DO** make it clear it is being provided under section 7 of the Data Protection Act and **DO** include the standard paragraphs [link to document in Objective removed] in your covering letter/email. No special transmission precautions are needed for open records.

Closed records

10.14 We can claim an exemption (at section 33(4) of the Data Protection Act) from the duty to provide personal data in response to a subject access request if the records are closed. This is because we consider we meet the conditions set out in section 33, namely:

- the records containing the personal data are being stored in a way that does not reveal the names of data subjects (note that this does not apply if the Catalogue reveals the names of the individuals)

- we are not causing substantial damage or distress to data subjects by just preserving the records

- the personal data is not being used to make decisions affecting the data subjects (note that any recall of the records by the department might affect this condition being satisfied)

However, as a matter of policy we will respond when the applicant has a real need of the information and it is practicable for us to do so, i.e. no open-ended search is required, and no other exemption prevents our doing so. This is because as a publicly funded institution we believe that we should, where possible, provide information necessary for people to claim their rights and entitlements, unless there is a reason not to do so (one of the exemptions at Annex 6 might be such a reason).

DO refer these requests to your manager in the first instance for a decision on whether to claim the exemption

DO consult the Deputy Data Protection Officer (YCT) if you think one of the exemptions at Annex 6 might apply.

10.15 If the applicant has not provided a document reference:

DO check that the request contains sufficient details for the requested personal data to be identified and located

If not, **DO** acknowledge their request and ask them to supply further details, using the standard paragraphs in Objective [link to document in Objective removed].

DO be as specific as possible about what details we need, e.g. which government body they worked for and the relevant dates, or what dealings they had with a government body that makes them believe we might hold their personal data

10.16 If they cannot or will not supply further details, we are not obliged to comply with the request – we do not have to undertake speculative searches.

DO consult your manager about whether to refuse the request on these grounds

If you are refusing, **DO** use the standard paragraphs in Objective [link to document in Objective removed] in your letter/email of refusal

10.17 Once it is clear what the applicant wants:

DO the usual searches of the Catalogue

If the request relates to a criminal court case, the names of those charged may have been removed from the catalogue entry and 'name withheld' inserted instead. **DO** check the spreadsheet with the original descriptions just in case [link to document in Objective removed].

10.18 If you find any relevant information, **DO** refer the request, with document details, to the FOI Centre.

10.19 As the records are closed we will also need to be satisfied that the applicant is entitled to the personal data. The FOI Centre will undertake the entitlement checks outlined at section 7. The FOI Centre will also levy the fee unless is it being waived (a fixed fee of £10 can be charged).

10.20 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 be taken after consultation with the relevant government department. This consultation will be handled through the FOI Centre in IMPD. See Annex 6 for information about exemptions in the Data Protection Act.

10.21 When providing the personal data:

DO make it clear it is being provided under section 7 of the Data Protection Act

DO include the standard paragraphs [link to document in Objective removed] in your covering letter/email

DO follow the guidelines on secure transmission at section 6

The right to seek correction or destruction of 'their' data

10.22 The Data Protection Act (section 14) gives data subjects a right to request correction or destruction of personal data relating to them but does not contain an absolute obligation on The National Archives to make corrections or destroy personal data within the archives whenever a request is received.

Correction

10.23 As a matter of policy, The National Archives will not make corrections unless required to do so by other legislation, by a court order, or when the Executive Team has decided that a correction should be made.

10.24 If corrections are made, it will be means of an addition to the record that leaves the original content intact and accessible, and the circumstances

will be documented. **DO** refer all requests for correction to the archives to the Data Protection Officer who will co-ordinate action. The Advisory Council will be informed of all such corrections.

Destruction

10.25 As a matter of policy The National Archives will not destroy personal data in the archives unless ordered to do so by a court. **DO** refer all requests for destruction to the Data Protection Officer who will co-ordinate action. The Advisory Council will be informed of all such destructions.

The right to complain about our use of 'their' data

10.26 The Data Protection Act (section 10) gives data subjects a right to complain about the way we are handling personal data relating to them. The most common examples of these complaints are that records about them have been opened, they are named within the web archive or they feature on our website or in the London Gazette.

10.27 The National Archives takes such complaints seriously and handles them in accordance with our published policy on takedown and re-closure. This policy is on our website – see http://www.nationalarchives.gov.uk/legal/takedown-policy.htm .

10.28 Complainants may not realise that they are exercising a right given them by the Data Protection Act but we must recognise cases and handle them in accordance with the Act. **DO** be alert to the possibility that complaints or comments may need to be handled as DPA s 10 cases.

10.29 **DO** refer s10 complaints as follows:

- Complaints about information on our or another website – Web Continuity, to mailbox webcontinuity@nationalarchives.gsi.gov.uk
- Complaints about original records – the FOI Centre in Information Management and Policy Department – to mailbox FOIcentre@nationalarchives.gsi.gov.uk
- Any other s10 complaints – to the Data Protection Officer, Linda Stewart

12 FURTHER INFORMATION AND ADVICE

For further advice **DO** contact the Data Protection Officer, Linda Stewart (extension 2537), or her deputies Michael Appleby (extension 2552) and Mark Hanvey (extension 5316). Their respective responsibilities are set out at section 2 of these procedures.

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 have slightly different requirements. These differences are drawn out in the procedures.

(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. Assume that anything on a computer falls in one of these categories.

(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 count as relevant filing systems but subject files containing occasional casual references to individuals do 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. This includes personal information in unstructured manual records such as subject files.

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

These categories of personal data must be treated with particular care.

Data controller

The person or body responsible for deciding what personal data is obtained and how it is to be used. The National Archives is data controller for personal data held by it or processed under its instructions but the Queen's Printer for Scotland (Carol Tullo) is data controller for personal data specific to that role.

Data subject

The person the personal information relates to.

Data Protection Officer

The person within The National Archives who takes the lead on providing advice and guidance on all aspects of data protection. This is currently Linda Stewart There are two Deputy Data Protection Officers, Michael Appleby and Mark Hanvey, whose remits are described at section 2.

Processing

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

ANNEX 2 DATA PROTECTION PRINCIPLES

The 8 Data Protection Principles require personal data to be handled as follows:

Principle 1	It shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
Principle 2	It 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
Principle 3	It shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
Principle 4	It shall be accurate and, where relevant, kept up to date
Principle 5	It shall not be kept for longer than is necessary for that purpose or those purposes
Principle 6	It shall be processed in accordance with the rights of data subjects under the Act
Principle 7	Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
Principle 8	It 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

ANNEX 3 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 personal data 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 comply with. (See Annex 2 for the principles). The Act also gives individuals rights of access to their own personal data, and prevents abuse of personal data by third parties.

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

Yes. All organisations, whether public or private, large or small, must process personal data in accordance with the Act. The National Archives processes a variety of personal data. Our corporate records contains personal data about visitors and our staff and others with whom we have dealings, such as journalists and contractors. The archives themselves also contain personal data; see section 10 for further guidance on personal data in the archives.

- **Are there any other rules that the National Archives must follow?**

Yes. We are also subject to HMG's *Security Policy Framework* which specifies methods for protecting personal (and other) data in government organisations.

- **What personal data is covered by the Act?**

All personal data that is recorded in some way is subject to the Act, whatever the technology used to collect and store it. This means all written documents, entries in databases, emails, CCTV footage or other video, audio cassettes and so on. Opinions about a person are included in the definition of personal data as well as factual details.

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

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

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

One way is by making a subject access request. Any person can make a subject access request; by writing to an organisation, asking to know what personal data is held, and what use is made of it. See Annex 5 to these procedures for how current staff can make subject access requests for their personnel files and other records.

To seek a correction you should write to the organisation pointing out the error, and where necessary, provide evidence that the personal data it holds is incorrect.

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

Yes. 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 and may be waived in other cases also. If in doubt, contact the Data Protection Officer or the Deputy Data Protection Officer (MA).

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

Only collect personal data which you really need and make sure that the person supplying it knows how you intend to use it. This is usually done by providing a Privacy Notice If you intend to add their details to one of our databases, such as the Customer Relations Management database, make sure people are given an opportunity to agree or disagree. Don't then use their personal data for any other purpose. This applies whether you are collecting the personal data on a form, over the telephone, or via the website or email. For full details, see section 3 of these procedures.

- **What is sensitive personal data?**

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

- **How should personal data be stored?**

Carefully! Keeping personal data 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. See section 6 of these procedures.

- **How long can I keep personal data?**

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. See section 5 of these procedures.

- **Can I give out personal data over the phone?**

Only with great care – consider the nature of the personal data and ensure the person on the phone has a right of access. See sections 7 and 8 of these procedures.

- **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.

- **Are there any particular rules to remember when sending out a mailshot by email?**

Yes. You should protect the privacy of recipients by ensuring that their names and email addresses are not visible to anyone else. If using Outlook, put all recipients' email addresses in the BCC box not the TO or CC boxes.

- **Can personal data be shared internally within The National Archives?**

You can share personal data with another part of The National Archives if it is to be used for a purpose that is similar to the purpose for which the personal data was originally collected. For example, if someone on a mailing list informs us of a change of address, we should also alter the address associated with their reader's ticket. But, unless the reader has given consent, we cannot use a record of which documents they have seen as an indication of their research interests and send publicity about forthcoming publications in the bookshop because that would count as a different use.

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

As a general rule we share personal data with other organisations only if the person has consented through a specific 'opt in' box. However, sometimes we have a contract with another body which requires us to share personal data with them. An example is Logica which does our payroll.

If personal data is managed on our behalf by external companies, it will be safeguarded by system operating procedures, approved by the Accreditor.

If you are planning to share personal data with another organisation and the data subject has not consented, you will need approval from the Director, Technology and Chief Information Officer. See section 8 of these procedures.

- **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 and we should correct it on request. See section 4 of these procedures.

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

The Freedom of Information Act extended the Data Protection Act to personal data 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 4 DATA SUBJECT ACCESS REQUEST FORM

1 Details of person requesting the information

Full name

Address

Tel. No. Fax No

Email address:

2 Are you the data subject? (Is the information about you?)

YES: If the information is about you, please supply evidence of your identity, i.e. something bearing your signature such as an original or copy driving licence or passport. If you are requesting CCTV please send also an up to date photograph. Original documents 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 us to identify the information you require. In particular, please specify whether you want information from the archives or our own business records. If you are requesting CCTV images from a visit to Kew please specify the date of your visit.

We may charge a fee for your application; an invoice will be sent to you if so.

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

I ……..(name) 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 National Archives must respond to your request within a period of 40 days. This period will not begin until your identity has been established and any relevant details received.

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)
- stamped addressed envelope for return of original proof of identity/authority documents

The National Archives will process the personal information included on this form in accordance with the Data Protection Act. The information will only be used in order to handle your request and will not be kept longer than is necessary to do so.

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

1.1 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 kept by HR

- 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, pre-Employment Health Declarations, sickness certificates and Occupational Health reports (if applicable), car park permit applications (if applicable), pension details and performance management forms. For Fixed Term Appointments the advertisement is filed also. The files also contain the outcome of basic clearances (unspent criminal record checks).

- Recruitment campaign files containing full documentation of recruitment, kept for up to 18 months for external audit purposes. (Some recruitment campaigns are in i-Grasp instead.)

Systems maintained by HR

- ResourceLink – HR's main information system, this contains detailed information such as home contact details, date of birth, job history and attendance details. Optimum is a linked system used for recording flexible working hours (replacing Atracs) and applying for and gaining approval of leave. There is a web-based interface (on Narnia) called MyView; it enables staff to check and to amend or request an amendment to their own details, and to access the time and attendance system. Optimum is also used to collect basic, non-sensitive data on "non-payroll" staff such as volunteers, contractors, agency temps and Professional Services staff, in accordance with Audit Committee requirements.

- i-Grasp (the e-recruitment system) – this is used to manage the recruitment process and includes applications, sift and boards reports and appointments. Relevant information about those appointed is put on manual files or in ResourceLink.This data is kept for 18 months for external audit purposes. The system also holds information about

people who express an interest in employment at The National Archives and are notified of vacancies. It is an opt-in system after a set period of inactivity. Anyone registered via our website receives an email after 28 days asking them if they still want us to hold their data, and if they do not respond their data is deleted.

- EPAYFACT – pay system run by Logica cmg (TNA's payroll provider) accessible by HR, containing pay data from 1 April 2003

Legacy systems kept but not added to by HR

- PROMISE/Compel – information system previously kept by HR, containing summary information including home address, date of birth, job history, absence, training and development details and recruitment campaigns. The data has been migrated to successor systems.

- Atracs – records of swipes on the flexi system. Once balances have been entered into ResourceLink, data from the previous 12 months will be kept for 6 months and then deleted.

Systems maintained by ICTD

- Websense – log of websites accessed by members of staff, including date, time and duration of visit; log of attempted visits to blocked sites and details of searches made on Internet search engines. Logs are overwritten after 90 days

- Telephony system – holds details of telephone calls made and received (including date, time, number dialled and duration and cost of call) for all telephones connected to the system, fixed and mobile. Reports can be run by ICTD. Call details are deleted after 12 months and voicemail messages are deleted after 31 days. The system also holds recordings of calls to specified enquiry lines in ARK, which are deleted after 2 months).

- Websense email security – log of incoming and outgoing emails, deleted after 30 days; quarantined messages (those identified as spam, phishin attempts or those containing profanity, deleted after one month; MessageLabs - another log of emails, maintained externally and deleted after 1 month; and Huntsman - record of email activity, deleted after 90 days.

- Outlook – email, schedules and contacts. Emails often contain personal data quite apart from the sender's and recipient's details. From July 2011 'sent' and 'calendar' items will be automatically deleted after 12 months. Emails generally are required to be either deleted when no longer needed or moved into Objective, with a relevant retention period, if there is a continuing business need for them. Information Asset Owners (IAOs) have a general responsibility to manage any risks resulting from inappropriate retention by their staff of personal emails within Outlook.

Information maintained by Security

- CCTV (Kew only) – Security maintains two digital CCTV systems. One system monitors and records images in the document reading rooms and invigilation room inside the building. The other system monitors and records internal and external areas including the perimeter, gates and grounds, and the museum and conference rooms. Images in both systems are deleted automatically after 31 days unless required for evidential purposes, in which case they are downloaded.

- Access control system – this records details of proximity passes issued, including the date or issue and expiry and by whom authorised, the pass holder's name, the controlled area the pass is used to access and the dates and times the pass was used. The information is deleted after 12 months.

Information about security clearances

- Estates keeps records of basic clearances, i.e. unspent criminal records checks, for contractors and volunteers. Applications and certificates are kept in files and destroyed 12 months after work has ended.

- The Departmental Security Officer keeps records for staff and contractors of National Security Vetting clearances, i.e. Security, Counter Terrorist and Developed Vetting checks. Clearances run for up to 10 years and can be extended, and the information is retained at least for the duration of the clearance. They include sensitive information.

Objective – material within the following functions:

- Human Resources:

    - Performance Management (7 years retention),

    - Attendance Management (sickness, leave and flex adjustments) (2 years retention),

    - Employee relations (disciplinary and grievance) 7 years retention. Expired warnings should be removed from files along with associated paperwork. Unproven allegations should be removed once investigation is completed

    - Work Experience (7 years retention).

    - Recruitment – job descriptions, reports and updates and audits (7 years retention)

    - Staff development – e.g. training course evaluation summaries, Further Education funding applications, training logs (3 years retention)

- Incidental references may occur elsewhere, e.g. within minutes of meetings

- Home (personal) folder – e.g. of managers. In addition, some managers occasionally keep printouts for a limited period.

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 Getting access to 'your' personal data

2.1 Your first step is to check MyView on NARNIA. This gives you access to information relating to you within HR's main system, ResourceLink. You can also update or amend some of the data in the system through MyView (see NARNIA for details).

2.2 If you want further personal data relating to yourself you should submit a subject access request. This 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.

2.3 If you are interested in particular personal data, e.g. information about yourself held in a specific system listed above or relating to a specific matter, you should describe the personal data you want. The more specific the request, the more effective the response will be.

2.4 If you want someone else to view the personal data on your behalf, or to accompany you when you view it, you should make this clear in your 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 and the individual must be named.

2.5 HR will not normally apply the standard £10 fee to subject access 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

3.1 Subject access requests will be handled by either the Human Resources Operations Manager (or the HR Information Systems Officer in her absence) or by the Deputy Data Protection Officer (YCT), depending on the nature of the information requested. Your request will be analysed to see whether any systems held outside HR are covered and, if so, the relevant people will be contacted. If the request is solely for CCTV it will be passed to

the Security Operations Manager to deal with in consultation with the Deputy Data Protection Officer (YCT).

3.2 All requests will be logged and tracked on a spreadsheet maintained by the HR Operations Manager, the HR Information Systems Officer and the Deputy Data Protection Officer. This is filed in Objective and accessible on a need to know basis.

4 Retrieval and assessment of personal data

4.1 For personal data within Objective, the KIM Team will provide a report listing items in Objective where you are named. The report can be configured to focus on certain files, dates or individuals, and may include the contents of Home Folders.

4.2 It is possible that some of the personal data requested will not be provided because it is subject to one or more of the exemptions in the Data Protection Act. For example, personal data might be exempt because it also relates to somebody else (i.e. another data subject) whose interests need protecting. The Deputy Data Protection Officer (YCT) will advise on the use of exemptions and oversee any redaction that is undertaken.

5 Provision of access to personal data

5.1 Access will be provided in one of these ways:

- By allowing you to view the material under supervision - this is how you will see the manual file kept by HR , who will make an appointment with you for this purpose. You can ask for copies at that time.

- by giving you a printout or a copy – for example, CCTV will be provided on a CD

- For personal data in Objective, HR will provide the report mentioned at section 4 above. If you want to access specific items listed in the report but cannot do so because of access privileges in Objective, the Human Resources Operations Manager will arrange access. Note that it may be necessary to redact content that relates to 3rd parties or is subject to an exemption (acting on the advice of the Deputy Data Protection Officer (YCT)).

- by emailing you a report from a database

5.2 If you are a Saturday worker this appointment can be either on the first Saturday morning of each month, when HR staff are present at Kew, or on another day by agreement.

5.3 If you have nominated someone else to view the personal data on your 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 your privacy.

6 Timescales

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

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

2 The Data Protection Act contains some exemptions that can (and in a few cases should) be claimed when a subject access request is received. The main ones relevant to TNA are:

- The date required has not been described sufficiently for it to be located or the applicant has not identified himself sufficiently for this entitlement to it to be verified (DPA section 7(3)).

- The data relates also to another person whose interests would be adversely affected by disclosure and has not given consent, and it is not possible to separate that person's personal data from that of the person making the subject access request (DPA section 7(4)).

- 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)

- For health information, educational records or social work records, where subject access would have an adverse effect on the data subject (SI 2000 No. 413)

- To avoid prejudicing regulatory activity by specified bodies (DPA section 31)

- the records are closed and processing is for historical or other research in compliance with specified conditions (DPA section 33)

- Information is available already under another Act (but not the FOI Act) (DPA section 34)

- Confidential references provided (not received) by TNA (DPA Schedule 7, paragraph 1)

- To avoid prejudicing combat effectiveness of the armed forces (DPA Schedule 7, paragraph 2)

- The data relates to assessing someone's suitability for appointment as a judge or a QC or award of an honour or dignity, e.g. an OBE or VC (Schedule 7, paragraph 3)

- To avoid prejudicing negotiations with the data subject (DPA Schedule 7, paragraph 7)

- A claim of legal professional privilege could be maintained in legal proceedings (DPA Schedule 7, paragraph 10)

3 If there is any possibility any of these exemptions might apply, **DO** consult the Data Protection Officer or the Deputy Data Protection Officer (YCT).