The National Archives

PROCEDURES FOR HANDLING PERSONAL INFORMATION UNDER THE DATA PROTECTION ACT 1998

Contents list

(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: nationalarchives.gov.uk/legal/privacy.htm .

1.2 The procedures apply to all personal data created or collected by The National Archives' 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), ResourceLink (the main HR system, succeeding Ciphr), Objective (our records management system) etc but can be found also in individual mailboxes and contacts lists in Outlook. They include systems managed on The National Archives' 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

2.1 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 Director, Technology, Chief Information Officer and Senior Information Risk Owner (Dr David Thomas) - accountable to Management Board and Executive Team for data protection.
- 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 **DOs** 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 The National Archives' 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's 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 third 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 (MA) 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 (MA) 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 (MA) 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 (MA).

8 SHARING PERSONAL DATA WITH THIRD PARTIES

This section explains how to handle requests for personal data from third parties who are not acting on behalf of the data subject, and also other proposals to share personal data with third 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 third 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 Police 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 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 third 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 The National Archives. 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.