

Instruction to NOMS HQ Staff on Freedom of Information and Data Protection

EXECUTIVE SUMMARY

STATEMENT OF PURPOSE	
This instruction explains the National Offender Management Service's policy on Freedom of Information and Data Protection and the procedures for complying with each.	
DESIRED OUTCOME	
To ensure compliance with the National Offender Management Service's statutory obligations under the Data Protection Act 1998 and the Freedom of Information Act 2000.	
PRISON SERVICE	
This instruction replicates the instructions contained in PSO 9020. Those PSHQ Groups which are compliant with PSO 9020 need take no further action in respect of this instruction.	
MANDATORY ACTIONS	
<i>All Heads of Areas/HQ Groups must appoint at least one 'Information Access Representative' (IAR).</i>	
RESOURCE IMPLICATIONS	
The amount of time spent by IARs on the new procedures required to comply with our statutory obligations under the Freedom of Information Act 2000 and Data Protection Act 1998 will vary from unit to unit. It is estimated that in most areas/units work on both procedures will amount to less than 5% of the IAR's conditioned hours.	
IMPLEMENTATION DATE:	1 st January 2005
(signed) Director: Peter Brook	

CONTENTS

Chapter 1 – Introduction

- 1.1. Purpose
- 1.2. Explanation of Terms
- 1.3. The Open Government Unit
- 1.4. Information Access Representatives
- 1.5. The Role of the Information Commissioner
- 1.6. The Powers of the Information Commissioner

PART 1: PROCEDURES FOR NOMS GROUPS/UNITS

Chapter 2 – Handling Requests under the Data Protection Act 1998 and Freedom of Information Act 2000

- 2.1. Identifying the Relevant Disclosure Regulations
- 2.2. General Principles for Handling Information Requests

Chapter 3 – Requests for Non-Personal Data

- 3.1. Handling Requests for Non-Personal Data
- 3.2. Initial Action upon Receipt of a Request
- 3.3. Procedures for Information Access Representatives

Chapter 4 – Requests for Personal Data

- 4.1. Handling Requests for Personal Data
- 4.2. Subject Access Requests (SARs)
- 4.3. Initial Action upon Receipt of a Request
- 4.4. Procedures for Information Access Representatives on Receipt of a Request
- 4.5. Subject Access Requests from (ex-) Staff: Medical Information
- 4.6. Ad Hoc Requests
- 4.7. Requests for Personal Information Relating to Ongoing or Prospective Legal Proceedings
- 4.8. Requests for Information from the Police and other Bodies
- 4.9. Exempt Information
- 4.10. Complaints

PART 2 – OUTLINE OF THE DATA PROTECTION ACT 1998 AND FREEDOM OF INFORMATION ACT 2000

Chapter 5 – The Legislative Framework of the Data Protection Act 1998 and Freedom of Information Act 2000

- 5.1. The Acts Together

Chapter 6 – Coverage of the Acts

- 6.1. Media and Source
- 6.2. Coverage of the Data Protection Act
- 6.3. Coverage of the Freedom of Information Act

Chapter 7 – Rights and Obligations

- 7.1. The Right of Access
- 7.2. NOMS Obligations under the Data Protection Act
- 7.3. Rights and Principles
- 7.4. Fit for Purpose
- 7.5. Accuracy and Amendments
- 7.6. Amendments to Personal Data Following a Subject Access Request

- 7.7. NOMS Obligations under the Freedom of Information Act
- 7.8. The Publication Scheme
- 7.9. What Information is on the Publication Scheme?
- 7.10. How can the Publication Scheme be Accessed?

Chapter 8 – The Right of Access

- 8.1. The Right of Access under the Data Protection Act 1998
- 8.2. The Right of Access under the FOIA
- 8.3. Our Obligations arising the Right of Access
- 8.4. The Environmental Information Regulations

Chapter 9 – Exemptions

- 9.1. Exemptions under the Data Protection Act
- 9.2. Exemptions under the FOIA
- 9.3. The Types of Exemptions
- 9.4. Dealing with Exempt Information

Chapter 10 – Document Security and Storage

- 10.1. Security
- 10.2. Storage

Annex A – Flowchart: Procedures for Handling Requests for Non-Personal Informations

Annex B – Flowchart: Procedures for Handling Requests for Personal Information

Annex C – Flagging and Feedback Procedures

Annex D – Subject Access Request Form: Staff

CHAPTER 1 – INTRODUCTION

1.1. Purpose

This instruction outlines the National Offender Management Service's (NOMS) policy in respect of two Acts of Parliament which entail fundamental changes to the way we work: the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FoIA).

The instruction is divided into two parts. The first part contains the procedures staff will have to follow in order to ensure compliance with both Acts, in particular it explains how to handle requests under each Act.

Part 2 contains background information on each Act and NOMS's wider obligations under them.

1.2. Explanation of Terms

The following terms are used within this instruction:

IAR	Information Access Representative
SAR	Subject Access Request
FoIA	Freedom of Information Act
OGU	Open Government Unit
EIR	Environmental Information Regulations
NOMS	National Offender Management Service

1.3. The Open Government Unit

Within the National Offender Management Service, the Open Government Unit is responsible for all Data Protection and Freedom of Information issues. The main duties of the Information Manager and the Open Government Unit (OGU) are to:

- Promote good practice within NOMS on Data Protection and Freedom of Information issues,
- Provide guidance and advice to all individuals be they employed or detained by NOMS or members of the public, on their rights and obligations as defined by the DPA and FoIA,
- Apply the requirements of the DPA and the FoIA consistently across NOMS,
- Act as the first point of call for complaints and grievances should an individual feel that NOMS has not fulfilled its statutory duty under the DPA or FoIA,
- Raise awareness, and
- Maintain the Service publication scheme. The publication scheme is a schedule of information NOMS publishes or will publish proactively and which is made readily available to the public.

The Open Government Unit can be contacted as follows:

Room 410
Abell House
John Islip Street
London SW1P 4LH

Information Line	020 7217 2125
Switchboard	
Fax	020 7217 5150
Website	www.hmprisonservice.gov.uk
e-mail	opengovernment@hmps.gsi.gov.uk

1.4. Information Access Representatives

Each NOMS Group/Unit must appoint at least one "Information Access Representative" (IAR). The Information Access Representatives will receive relevant training shortly after appointment and then as and when necessary.

When an IAR moves to another part of the organisation or leaves NOMS OGU must be informed and a new IAR appointed.

IARs must work with OGU to ensure that NOMS meets its obligations under the DPA and FoIA. This will usually include the following:

- Liaising with OGU on disclosure issues.
- Providing a local source of expertise on the DPA and FoIA.
- Handling simple requests for information locally.
- Identifying and forwarding to OGU more complex, large or sensitive requests for information and those with a scope beyond their local policy/operational area.
- Duplicating and forwarding requested information to OGU in respect of requests under both Acts.
- Upholding and applying record management procedures in their areas, for example weeding schedules.
- Ensuring compliance with each Act as they deem necessary and upon advice from OGU by, for example, amending incorrect information and helping OGU satisfy complaints from requesters.

1.5. The Role of The Information Commissioner

The Information Commissioner is an independent officer who reports to Parliament. His main duties are:

- To provide guidance and advice on how organisations should meet the statutory requirements of the DPA and FoIA.
- To encourage compliance with the Codes of Practice issued by the Department for Constitutional Affairs in accordance with the FoIA.
- To provide guidance and advice to individuals on their rights under both Acts.
- To enforce compliance with both Acts.

1.6. The Powers of The Information Commissioner

The Information Commissioner has a number of powers available to him for the purposes of enforcing compliance with both Acts.

Should the Information Commissioner wish to ascertain whether or not NOMS has been in compliance with either Act he can issue an "Information Notice." This specifies information, recorded or otherwise, *which we must provide in order for the Commissioner to come to a decision.*

If NOMS fails to meet its obligations under either Act, the Commissioner can impose an "Enforcement Notice" which details the steps which *must* be taken in order to reach compliance. There is no upper limit on the cost of complying with an Enforcement Notice.

Failure to comply with either an Information Notice or an Enforcement Notice can result in the Commissioner informing the High Court who may choose to treat the non-compliance as a contempt of court.

The Commissioner can seek to obtain a warrant to inspect the premises of an organisation he believes not to be in compliance with either Act and seize materials.

The Commissioner can bring criminal proceedings resulting in a fine against organisations (or their employees) who deliberately amend or destroy information in order to prevent it being disclosed in the event of a legitimate request for it under either Act.

The Information Commissioner can be contacted as follows;

Information Commissioner

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Information Line	01625 545745
Switchboard	01625 545700
Fax	01625 524510
Website	www.informationcommissioner.gov.uk
e-mail	mail@ico.gsi.gov.uk

PART 1:

PROCEDURES FOR NOMS GROUPS/UNITS

CHAPTER 2 – HANDLING REQUESTS UNDER THE DATA PROTECTION ACT 1998 AND FREEDOM OF INFORMATION ACT 2000

2.1. Identifying The Relevant Disclosure Regulations

Requests for information relating to a living, identifiable individual are covered by the Data Protection Act 1998 and should be handled according to its provisions. Any requests for information which do not fall into this category should be handled in accordance with the Freedom of Information Act 2000.

The NOMS procedures for handling information covered by the Data Protection Act are described in Chapter 4 and Annex B. The correct procedures for handling requests for information covered by the Freedom of Information Act should be handled in accordance with Chapter 3 and Annex A.

The Data Protection Act does not cover information held on the deceased and therefore the procedures for handling requests for this type of information are found in Chapter 3, not Chapter 4.

Any requests which include a mix of information covered by the two Acts must be forwarded to OGU immediately.

2.2. General Principles For Handling Information Requests

Requests for information must either be met, or forwarded to OGU as soon as possible. While the DPA and The FoIA stipulate maximum deadlines, they also state that requests should be answered sooner if possible.

Requests for information must only be refused or part refused by OGU. If a request is received which it is believed ought to be refused it should be forwarded to OGU immediately

If necessary, requesters should be given help in making their requests including refining them to cover the information they actually want. If requests are received by telephone, the requester should be given OGU's address if necessary.

Handling requests for information using the formal procedures described in this instruction can be expensive and time consuming but is often necessary to ensure compliance with the DPA or FoIA. Therefore, straightforward and simple requests for information should be handled promptly at the point of receipt without resorting to the formal procedures.

Your local IAR can advise on the best method for handling particular requests.

All monitoring of FoIA requests handled by NOMS will be carried out centrally. There is no requirement for units to carry out their own monitoring.

When NOMS units receive requests for information via CTS which they refer to the OGU, they must first remove them from the system to ensure that they are not double-counted (once by CTS, once by OGU). Advice on how to remove cases from the CTS system can be sought from the OGU or HO DCU.

NOMS units must never record cases as FoIA requests on the CTS system. Requests which fall under the "simple" category (see section 3.3) should be handled as normal correspondence on CTS; non-simple cases will be monitored by the OGU as explained above.

CHAPTER 3 –REQUESTS FOR NON-PERSONAL DATA

3.1. Handling Requests For Non-Personal Data

Any request for information not covered by the DPA (i.e. which does not contain information on a living, identifiable individual) is covered by the FoIA and should be dealt with as follows. See 3.3.2 for more information on what qualifies as a FoIA request.

These procedures are not designed to interfere with the day-to-day exchange of information between NOMS and the public, staff, offenders, the press or any other body. Staff should treat such requests for information in exactly the same way as before the Act came into force.

Refer to Annex A for a flowchart detailing the steps which need to be taken for handling a request for non-personal information/data.

3.2. Initial Action Upon Receipt of a Request

Any request for information which does not fall into the “day-to-day” category should in the first instance be referred to your unit’s Information Access Representative. *Due to the 20 day limit requests must be met or referred without delay.*

3.3. Procedures for Information Access Representatives

If a request is received for information on the publication scheme the requester should be informed of this along with details of how to access the scheme.

On receipt of a request for information it should be ascertained whether it meets the minimum requirements to be covered by the FoIA. It must:

- Be made in writing (including electronic means, e.g. e-mail or fax)
- Be received in legible form
- Be usable for subsequent reference
- State the name and a correspondence address for the requester
- Describe the information requested

It does NOT have to refer to or name the FoIA to constitute an FoIA request.

If the request does not meet these requirements then the IAR should decide whether or not it would be appropriate to comply with the request anyway. It would be appropriate, for example, if the request would be simple and straightforward to comply with and is for information which the IAR has immediate access to, and has no concerns over disclosing.

If the request does not meet the requirements and the IAR is not happy to comply with it, then he should inform the requester of this, advise them on how to make a full, written request and to address it to OGU. It is NOMS’s duty under the Act and the Code of Practice issued by the Department of Constitutional Affairs (9.3.5, 8.7.3) to aid (potential) requesters with their requests.

If a request is received by an IAR and meets the requirements of the Act then the IAR must answer it within 20 working days unless:

- The request is for a large amount of information
- The request may require a fee to complete.
- The IAR does not have immediate access to all of the information requested

- The IAR has concerns over disclosing the information or believes any part of it may be covered by an exemption.
- Additional information is required to complete the request

If any of the above are the case then the IAR should forward the request to OGU immediately.

If the request is handled locally and/or by the IAR, a fee must not be charged.

If some, but not all, of the information is held by the IAR's area/group then the IAR should forward that information to OGU along with the request.

In the event of a request being received by OGU they will, if necessary:

- Determine a fee and issue a fees notice.
- Request additional information from the requester.

Subject to 3.3.8 OGU will collate the information via the appropriate IAR(s) and apply any relevant exemptions.

Once OGU has completed the request it will be despatched to the requester.

CHAPTER 4 - REQUESTS FOR PERSONAL DATA

4.1. Handling Requests for Personal Data

On receipt of a request for non-personal data (information which is not about an identifiable, living individual), please refer to Chapter 3 or Annex A

These procedures are not designed to interfere with the day-to-day disclosure to staff and offenders of their personal information. See 4.9, "*Ad hoc Requests.*"

In general, an individual's personal data should not be disclosed to a third party without the individual's written consent. *Requests for an individual's personal data from a third party must always be referred to OGU or your local Information Access Representative.*

The Act does not prohibit or limit the disclosure of information within the Home Office or its agencies.

NOMS may exchange personal information without the subject's consent to agencies with which there is an agreed protocol (e.g. the Police, see 4.11) or when required to do so by law (e.g. the courts, see 4.10).

Annex B contains a flowchart detailing the steps which need to be taken in order to handle a request for personal information/data.

4.2. Subject Access Requests (SARs)

Under section 7 of the DPA individuals, ("data subjects") are entitled to access any or all of the personal information held on them by the National Offender Management Service. *For a request to constitute a "subject access request" the subject must present the following:*

- *The request in writing, signed by them.*
- *A £10 fee.*

A proforma for use by staff to make requests can be found at Annexes D and E respectively. This is intended to simplify the process but it should be noted that requests simply have to be in writing to meet the criteria of the Act.

Such a request may be made on behalf of a subject (e.g. by a solicitor or family member) provided it contains the fee and the signed authority of the subject to disclose their information to that person (see 4.10).

OGU will co-ordinate all SARs with the assistance of the relevant IARs.

"Formal" Data Protection Act requests, i.e. those which meet the criteria for an SAR must always be handled by OGU.

OGU will only fax requests for personal data relating to SARs when the appropriate fee and written authority have been received.

NOMS areas/groups must not charge a fee for processing an SAR. This will always be done by OGU.

In most cases it is NOMS policy to meet a subject's rights under the DPA by supplying them with a copy of the information held on them. OGU may however choose to facilitate access by another

method if providing a permanent copy would involve “disproportionate effort.” This does not permit NOMS to deny a request; *an SAR must always be met by one method or another.*

4.3. Initial Action Upon Receipt of a Request

If a request for personal data is received which fulfils the criteria for a subject access request it must be forwarded to your local IAR immediately.

If a request is received which does not meet the criteria for an SAR, it may be appropriate to answer it anyway based on its size, scope and content. Please see 4.9 “*Ad hoc Requests.*”

If a request is received which does not fulfill the criteria for an SAR and which you are unable to answer or have reservations about answering, please contact your local IAR or OGU for advice.

4.4. Procedures for Information Access Representatives On Receipt of a Request

On receipt of a request which meets the criteria for an SAR, it must be forwarded to OGU immediately even if could be answered locally. Please collate any locally held information covered by the request and forward to OGU as soon as possible. OGU will fax to confirm what information is required.

If the IAR receives a request for personal data which does not constitute an SAR it should be answered locally unless:

- It is complex or for a large amount of data.
- It is likely to cover data held outside your area or group
- You have reservations about disclosing the requested data or are uncertain of the legal/policy position.

If any of the above are the case, forward the request to OGU immediately. See 4.8 for more information on answering requests for personal data locally.

Wherever possible, subjects should be aided in making their requests. For example, by advising on the requirements for an SAR or by suggesting an *ad hoc* request if in your judgement that would be more appropriate.

4.5. Subject Access Requests from (Ex-) Staff: Medical Information

On receipt of an SAR from an (ex-) member of staff OGU will fax the relevant units stating the information required.

Medical information held on a personnel file should only be released with the authority of the medical practitioner who originally compiled it.

Medical information from firms providing occupational health advice to NOMS should be forwarded to the originating office for them to decide whether or not it should be disclosed. The office in question should be instructed by the IAR to return any disclosable information copied, sealed and marked “Medical in Confidence” along with the original file.

Once returned, any disclosable information from the occupational health advisers should be forwarded to OGU immediately.

4.6. Ad Hoc Requests

The procedure for handling an SAR should not interfere with reasonable requests from staff or offenders for limited access to personal information held on them.

In most cases it would be appropriate to meet the following sorts of requests informally:

- Requests from staff to see their pay history.
- Copies of Annual Reports, leave sheets or other information to which the member of staff has already been party.

Although small requests should be met without charge, reasonable copying charges may be made.

Ad hoc requests for information which refers to third parties or raises concerns for other reasons should be forwarded to your local IAR or OGU.

If in doubt, contact OGU or your local IAR for advice.

4.7. Requests for Personal Information Relating to Ongoing or Prospective Legal Proceedings

Non-SAR requests from solicitors or other legal representatives in relation to legal proceedings should be dealt with outside of the normal DPA process. The DPA allows disclosure of personal data to third parties when done so in connection with legal proceedings. If in doubt, seek advice from OGU.

Requests for information on individuals by the courts should in most cases be met locally.

In the event of such a request, staff should satisfy themselves that the proceedings are genuine and that the requested information is relevant to them.

There is no legal requirement to make such a disclosure in the absence of a court order. However, insisting on a court order should be avoided as the National Offender Management Service can be penalised on costs if the court considers that they were being obstructive in not responding to a disclosure request.

Unnecessary delays in meeting reasonable requests will often result in a court order being issued.

Reasonable and relevant requests for information relating to the individual the legal professional represents should be met where possible. Where possible, any information relating to other individuals (e.g. other staff) should be removed.

Areas/groups may charge a reasonable fee for copying the information.

Requests for an individual's entire record (or similar) when connected to legal proceedings should be treated with caution and referred to OGU.

Requests for personal data relating to an individual other than the legal professional's client should be referred to OGU.

It should not normally be required to contact the Treasury Solicitor direct. If legal advice is required this will be arranged by OGU. *If a Court Order is served upon an area or unit it must be complied with by the date given.* Failure to comply with the order on time may result in NOMS or its staff being held in contempt of court.

4.8. Requests for Information from the Police and Other Bodies

Requests for information from the police and other bodies should also be dealt with in line with existing practice.

The exchange of personal data between the police and the Prison Service is governed by the *Memorandum of Understanding – Association of Chief Police Officers and HM Prison Service* (February 2002).

The Memorandum of Understanding is updated from time to time. The most recent version can be obtained from the Police Advisor's Section.

Advice on disclosures to the Police in line with the Memorandum of Understanding can be sought from the Police Advisor's Section on:

- Tel: 020 7217 6614 (24hrs)
- Fax: 020 7217 6592

Advice on disclosures from other parts of NOMS HQ to other bodies, e.g. local authorities and other government agencies or departments, can be sought from OGU.

4.9. Exempt Information

With the exception of medical and security information, OGU will vet all personal data in line with the DPA 1998 before releasing it to the subject.

Any request for information to which it is believed an exemption may apply must be handled by OGU.

With the exception of medical information, information must not be, edited, deleted or otherwise amended before being supplied to OGU.

Any information which raises concerns in terms of disclosure should be flagged up using the flagging procedure outlined in Annex C.

4.10. Complaints

OGU will handle all complaints made by staff or prisoners in relation to SARs or NOMS's wider obligations under the DPA.

OGU will also deal with assessments or enquiries from the Information Commissioner's Office.

Any complaints or indications of legal challenges relating to the DPA should be referred immediately to OGU.

PART 2:

OUTLINE OF THE DATA PROTECTION ACT 1998 AND FREEDOM OF INFORMATION ACT 2000

CHAPTER 5 – THE LEGISLATIVE FRAMEWORK OF THE DATA PROTECTION ACT 1998 AND FREEDOM OF INFORMATION ACT 2000

5.1. The Acts Together

Together, the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FoIA) represent a comprehensive right of access to information held by the National Offender Management Service, other public bodies and some private companies (particularly in the case of the DPA).

The Acts are designed to increase the transparency of the decision-making processes which affect both individuals (DPA) and wider society (FoIA).

Both Acts change the default position from one of secrecy to disclosure with the balance being heavily in favour of the latter.

The Acts do not provide a right of access to *all* information held by NOMS. Each contains a system of exemptions which are explained in Chapter 10.

CHAPTER 6 – COVERAGE OF THE ACTS

6.1. Media and Source

The FoIA and DPA apply to their respective types of information, regardless of the media on which they are recorded. This includes, but is not limited to, registered and unregistered manual records, electronic records, e-mails, handwritten notes, drafts and even post-it notes.

The Acts apply to their respective types of information regardless of their source or “owner.” For example, information received from the police or other organisations. NOMS is responsible for its own compliance with the Acts and *must*, if required, disclose information originating from other organisations irrespective of their wishes.

These obligations apply equally to other public authorities receiving NOMS information. This *must* be borne in mind when transferring information outside the organisation.

6.2. Coverage of the Data Protection Act

The DPA applies to all recorded personal data held by the National Offender Management Service. Personal data is defined as any of the following which refers to a living, identifiable individual:

- Factual information;
- Expressions of opinion;
- Indications of intent (by the organisation holding the data or otherwise).

The Act also defines “sensitive personal data” to which additional parts of the Act apply. Sensitive personal data is data which relates to a living, identifiable individual's:

- ethnic origin;
- political opinions;
- religious or other beliefs;
- trade union membership;
- physical or mental health;
- sexual life;
- offences;
- criminal proceedings and sentencing.

NOMS processes large amounts of personal and sensitive personal data. The term “personal data” includes “sensitive personal data.”

The term “process” is wide ranging. It covers almost any action taken in respect of personal data from initial collection and recording through to handling or manipulation and eventual destruction. It also covers the actions of merely holding or retaining personal data.

6.3. Coverage of the Freedom of Information Act

The FoIA applies to all recorded information held by NOMS which is not covered by the DPA.

All such information *must* be considered for disclosure in the event of a request for it and may only be withheld if it is covered by an exemption from within the Act.

The FoIA and DPA are “blind” to protective markings. Information marked “restricted”, “confidential” etc can only be withheld if it is covered by an exemption. (See Chapter 10).

CHAPTER 7 – RIGHTS AND OBLIGATIONS

7.1. The Right of Access

Each Act confers a right of access to particular types of information. The right of access under both Acts is covered in Chapter 9.

The procedures for handling requests for information under the FoIA and DPA are detailed in Chapters 3 and 4 respectively.

7.2. National Offender Management Service Obligations Under the Data Protection Act

The Data Protection Act not only confers on individuals a right of access to the personal data held about them but obliges the National Offender Management Service (and other organisations) to process such information fairly.

It is critical that disclosures to third parties are not made inappropriately and in breach of the DPA. In practice, this will often mean that NOMS *must* not disclose personal data on any individual to a third party without the data subject's explicit consent. However, personal data may be disclosed to third parties when it is necessary to carry out NOMS's functions and/or when there is an agreed protocol in place to govern it, e.g. with the police (4.11).

Under some circumstances NOMS is required to make disclosures of personal data to third parties by law, e.g. to the courts. Under these circumstances we can do so without breaching the Act (4.10).

7.3. Rights and Principles

Any individual on whom personal data is held enjoys seven rights under the DPA. These are the:

- right of subject access,
- right to prevent processing likely to cause damage or distress,
- right to prevent processing for the purposes of direct marketing,
- rights in relation to automated decision-taking,
- right to take action for compensation if the individual suffers damage by any contravention of the Act by the 'data controller',
- right to take action to rectify, block or destroy inaccurate data, and
- right to make a request to the Information Commissioner to assess if any provision of the Act has been contravened.

The DPA also lays down eight principles which govern how organisations may use personal data. These are that personal data *must* be:

- processed fairly and lawfully,
- processed for limited purposes,
- adequate, relevant and not excessive in relation to the purposes for which they are recorded,
- accurate and kept up to date,
- kept no longer than is necessary,
- processed in accordance with the data subject's rights under the Act,
- kept secure and protected against loss or damage, and
- adequately protected if transferred to countries outside the European Economic Area.

For the definition of processing see 7.2.5.

The rights and principles are subject to limited exemptions which are explained in Chapter 10.

Advice on whether a particular course of action is compliant with the DPA rights and principles can be obtained from OGU.

7.4. Fit for Purpose

The DPA obliges organizations to notify the Information Commissioner of the purposes for which they will process personal data. This Notification must be approved by the Commissioner.

Personal data collected by NOMS may only be used for these purposes and no other. Our current uses/requirements are covered by the Notification.

NOMS has a duty to inform individuals of the purposes for which we intend to process their personal data when we first begin our dealings with them. E.g. when an individual applies for a job/starts employment.

7.5. Accuracy and Amendments

The DPA obliges NOMS to keep all personal data, no matter how seemingly insignificant, accurate and up to date.

Care should be taken when transferring personal data from one system (manual or electronic) to another.

If the same data is held on multiple systems (manual or electronic) then it *must* be consistent across them all.

Individuals may contest the accuracy of the personal data we hold on them. If they can provide proof of the inaccuracy we are obliged to amend or delete the incorrect information as appropriate.

If the accuracy of the information cannot be clearly proven or disproven we are obliged under the DPA to note on the record that the information in question is in dispute.

7.6. Amendments to Personal Data Following a Subject Access Request

Following a subject access request (see Chapter 4) only routine amendments may be made to the requested data between the request being made and the information being provided to the subject. That is, amendments which would have been made irrespective of the request.

Under no circumstances *must* information be altered or deleted for any reason arising from a request being made, before the information is provided to the subject.

7.7. National Offender Management Service Obligations Under the Freedom of Information Act

The FoIA does not regulate the use/handling of the information it covers as the DPA does for personal data.

Section 46 of the FoIA however provides for a Code of Practice, issued by the Department for Constitutional Affairs (DCA), detailing best records management practice. A copy of this code can be obtained from the DCA website or from OGU.

The FoIA also provides for a Code of Practice (again issued by the DCA) under section 45 which details how public authorities can best go about discharging their obligations under the Act.

The focal point of the FoIA, the right of access is covered in Chapter 9.

7.8. The Publication Scheme

Under the FoIA, each public authority *must* produce a publication scheme, a schedule of information to be made readily available. It *must* ensure that it publishes information in accordance with it.

The Home Office publication scheme, including NOMS's, was approved by the Information Commissioner in October 2002.

7.9. What Information is On the Publication Scheme?

The publication scheme does not list the actual documents, or items of information which will be published in accordance with it. These can be changed from time to time according to the scheme.

The publication scheme lists *types* of information for which there is a high demand anticipated and that for which there is an obvious public interest in disclosing.

The publication scheme states by what method the information on it is available and the charges made for disclosing it.

7.10. How Can the Publication Scheme Be Accessed?

The contents of the NOMS publication scheme, and the scheme itself, can be accessed via the website. Enquiries for information on the publication scheme from those without Internet access should be forwarded to OGU who will advise the requester as appropriate.

CHAPTER 8 – THE RIGHT OF ACCESS

8.1. The Right of Access Under the Data Protection Act 1998

The DPA entitles individuals to receive in intelligible (legible and understandable) form any personal data held on them by NOMS.

An individual can access this right by making a “formal” **subject access request**. The necessary criteria for making such a request along with the procedure for handling one can be found in Chapter 4.

This right is subject to limited exemptions as covered in Chapter 10.

Usually the right of access *must* be met by providing the data subject with a permanent copy of the personal data requested. See 4.2.8.

The right of access under the DPA only applies to information held on the individual making the request.

A fee may be charged for complying with a request. OGU charges the maximum fee of £10 for all subject access requests.

Subject access requests *must* be completed as soon as possible, within a maximum of 40 calendar days.

NOMS does not have to comply with requests which have been repeated within an unreasonably short length of time.

While OGU encourages *ad hoc* disclosures (see 4.9) it should be noted that an individual's right of access is not conferred unless a formal subject access request is made (see Chapter 4).

Ad hoc disclosures are therefore made at local discretion.

8.2. The Right of Access Under the FoIA

There is no such thing as a distinct “Freedom of Information Act Request.” **Any** request for non-personal information/data made to the National Offender Management Service is covered by the Act providing it meets the criteria set out in 3.3.2.

The right of access under the FoIA is not limited to any type of person or organisation, or by nationality.

8.3. Our Obligations Arising From The Right Of Access

A person making a request for information is entitled to be told in writing:

- Whether or not we hold the information requested
- If so, to be supplied with it, subject to exemptions.

The requester may express a preference as to how the information should be communicated, e.g. a copy of the information (paper or electronic), a summary of the information or the opportunity to inspect the information where held. NOMS is obliged to consider the requester's preference though may choose to communicate the information differently if reasonable.

NOMS may charge a fee for processing the request (see Chapter 3).

NOMS *must* comply with a request for information as soon as possible, within a maximum of 20 working days of receipt. (See Chapter 3)

NOMS is obliged to assist (potential) requesters with their requests by helping them to identify the information they seek and if necessary, by helping them with the process of making a written request.

NOMS is not obliged to comply with requests which are deemed to be “vexatious” or which repeat a previous request by the same individual within an unreasonably short length of time. The term “vexatious” is not defined in the Act.

8.4. The Environmental Information Regulations

The Environmental Information Regulations (EIRs) provide for a third information access regime limited to environmental information.

The EIRs are not covered by this instruction.

Information on the regulations and the handling of requests made under them can be sought from:

The Sustainable Development Co-ordinator,
Room 501
Abell House
John Islip Street
London
SW1P 4LH

Tel: 0207 217 5435

CHAPTER 9 – EXEMPTIONS

9.1. Exemptions Under the Data Protection Act

The DPA provides a number of exemptions to the rights and principles outlined in Chapter 8.

In particular, certain information is exempt from disclosure to the data subject in the event of a subject access request being made.

Very little personal data held by NOMS is exempt from disclosure. It should be assumed that any personal data held by NOMS is potentially disclosable.

NOMS is not obliged to disclose information about third parties in the event of a subject access request. This will be edited out prior to disclosure (though see 10.1.5). The most common exemptions to the right of access relied upon by NOMS are:

- Information is exempt from disclosure if doing so would prejudice the prevention or detection of crime.
- Information is exempt from disclosure if it is legally privileged, e.g. comprises legal advice given to NOMS.

NOMS staff are not considered by the Information Commissioner or the courts to be “third parties.” Their names or identifying information, when recorded in a professional capacity, are only exempt when there is a reasonable expectation that “bodily safety or even life itself are put at risk” through disclosure.

Only OGU should apply exemptions to disclosures of personal data. Application of exemptions by area/group staff can lead to unnecessary legal challenges and therefore costs (see 4.5.9 and 4.12.3)

Should an IAR or other member of staff wish to alert OGU to information which they believe to be exempt when handling a request they should made use of the flagging procedure at Annex C.

9.2. Exemptions Under the FoIA

Very little of the non-personal information held by NOMS is covered by an FoIA exemption. It *must* be assumed, unless indicated otherwise by OGU or your local IAR, that any given piece of information held by NOMS will be disclosable.

The FoIA is “blind” to protective markings. Documents carrying such markings may only be withheld if covered by an exemption.

9.3. The Types of Exemptions

The exemption regime in the FoIA is complex. The exemptions fall broadly into two categories: the absolute and the qualified.

When an absolute exemption applies to a requested piece of information, NOMS can withhold that information.

An example of an absolute exemption is Section 40 which applies to personal information (dealt with in the DPA). If, for example, an individual makes a request for the personal information of an offender or member of staff (other than themselves), NOMS can withhold the information.

When a qualified exemption applies to a requested piece of information, NOMS may only withhold the information if the public interest in withholding it outweighs the public interest in disclosing it. If it does not, the information *must* be disclosed as normal.

In exceptional circumstances NOMS is not obliged to inform a requestor whether they hold a requested piece of information.

Of the information held by NOMS which is exempt, the vast majority will fall under a qualified exemption.

An example of a qualified exemption is Section 30 which allows for the non-disclosure of information relating to “law and order.” Therefore, information which if released might prejudice the “apprehension or prosecution of offenders” is exempt. If however, the public interest in disclosure is so great as to outweigh the public interest in preventing or detecting the related crime(s), the information *must* be disclosed.

“The public interest” is not the same as “what interests the public.”

9.4. Dealing With Exempt Information

If you receive a request for information which you believe may be exempt, or you have other reasons for believing should not be disclosed, forward the request to OGU.

Exemptions should only be applied to requested information by OGU. Inappropriate application of exemptions is likely to lead to unnecessary legal challenges or the intervention of the Information Commissioner.

CHAPTER 10 – DOCUMENT SECURITY AND STORAGE

10.1. Security

Only those who need access to particular information in order to carry out their work should be allowed it.

NOMS has a legal obligation to ensure that only those who need access to personal and sensitive personal information are allowed it. Electronic or manual systems which contain personal data should include appropriate technical measures to protect against unauthorised access.

The DPA states that appropriate organisational measures should also be in place to protect (sensitive) personal data. Manual records or computer printouts *must* not be left on desks overnight and PCs *must* be logged off when not in use.

10.2. Storage

All NOMS documents should be stored where they are protected from physical damage. When determining areas/methods used for storing information consideration should be given to potential damage from environmental factors.

Ideally, areas used for storing records should be used for that purpose only. If this is not possible, care should be taken to ensure that records are not damaged by other uses of the area.

“Live” records of any type should be stored in a system which facilitates easy retrieval.

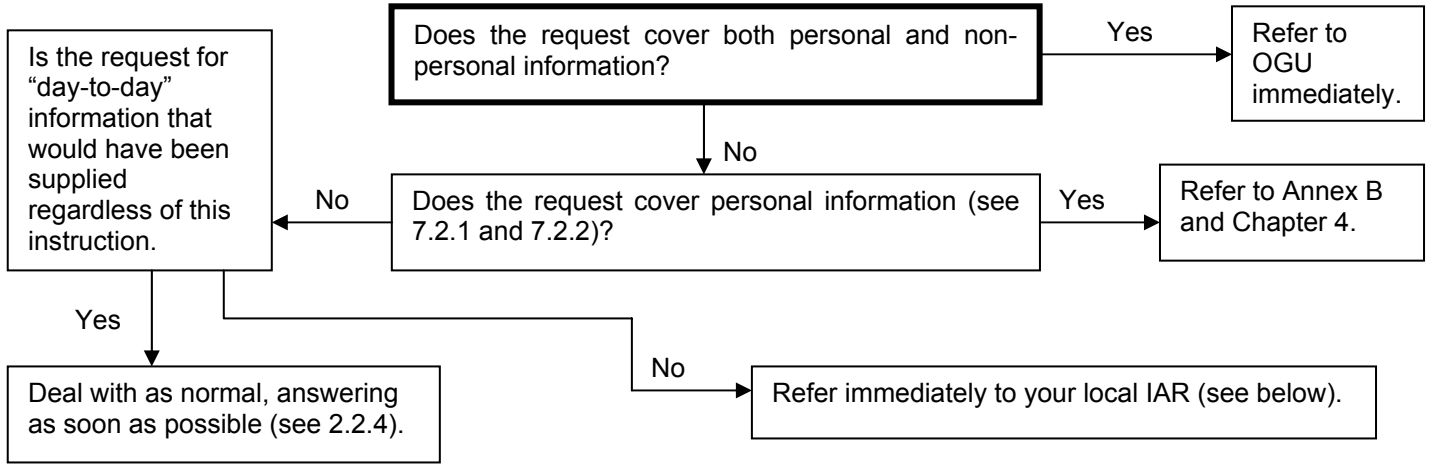
“Dead” or “dormant” records should be stored in destruction date order.

Systems should be in place to track the movement of all types of records.

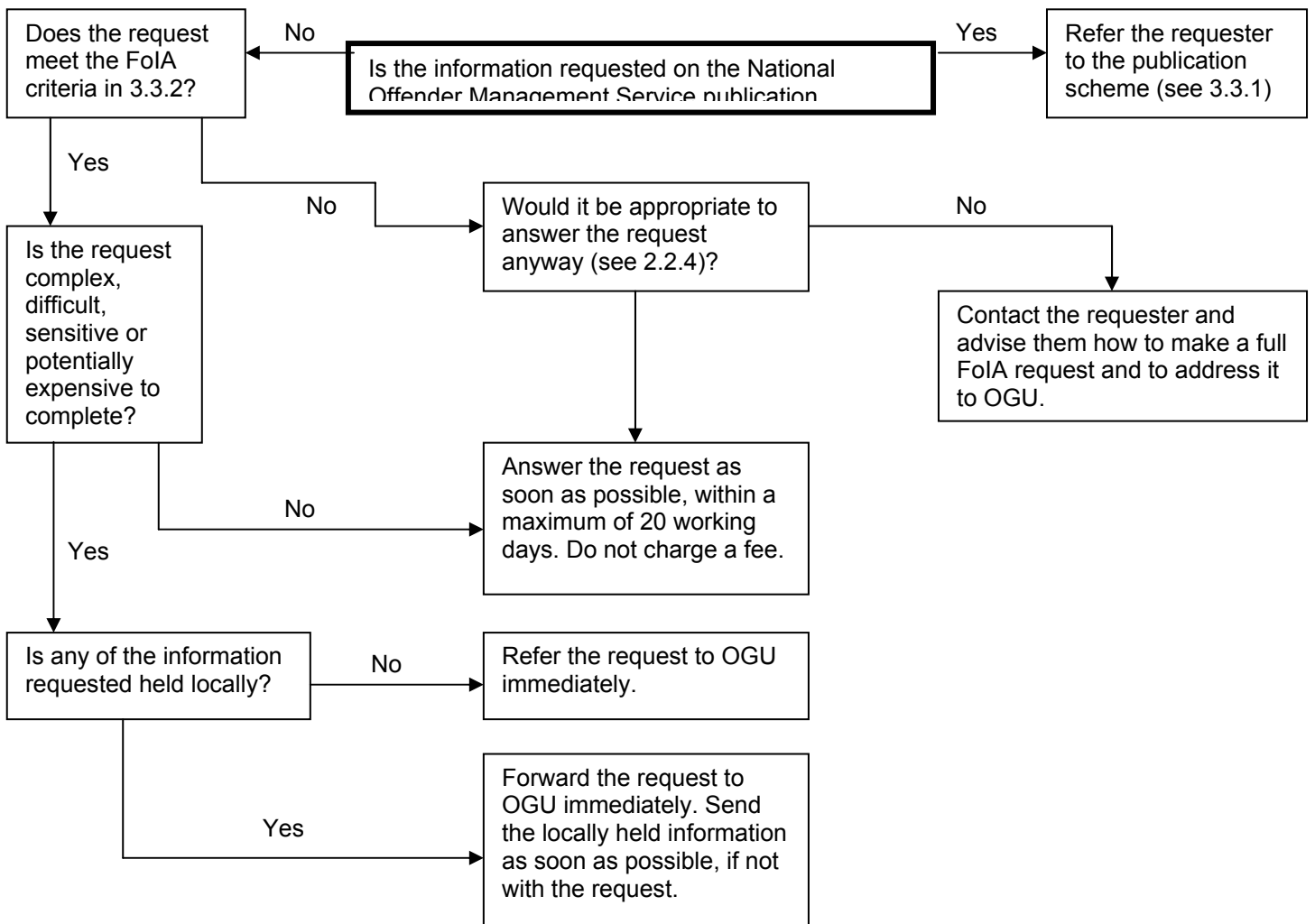
ANNEX A

FLOWCHART: PROCEDURES FOR HANDLING REQUESTS FOR NON-PERSONAL INFORMATION

1. PROCEDURES FOR ALL STAFF



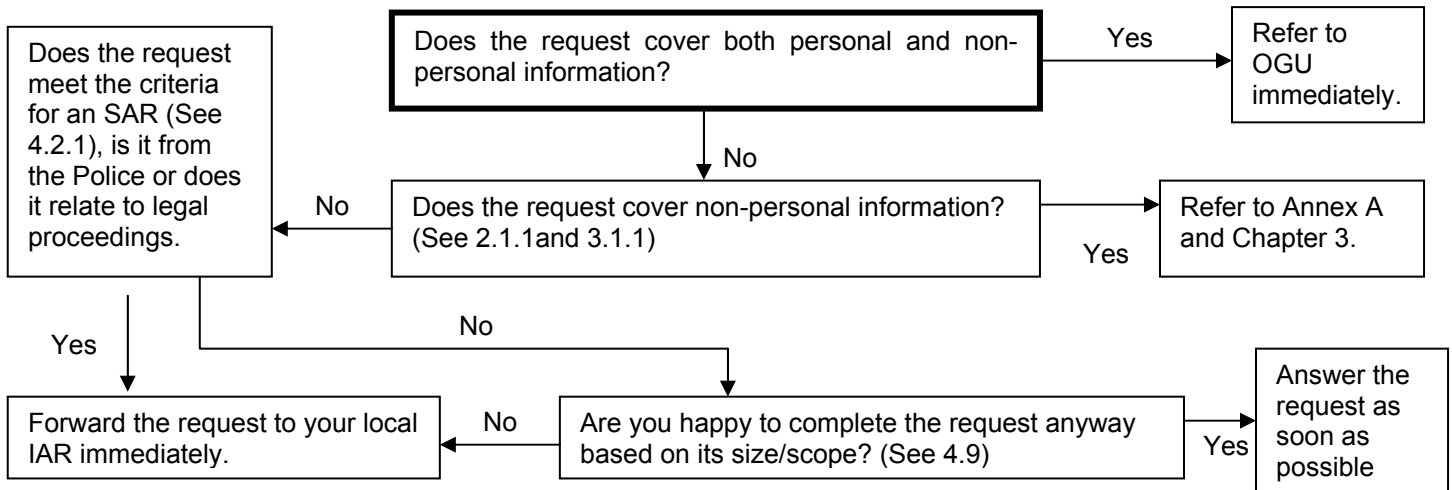
2. PROCEDURES FOR IARs



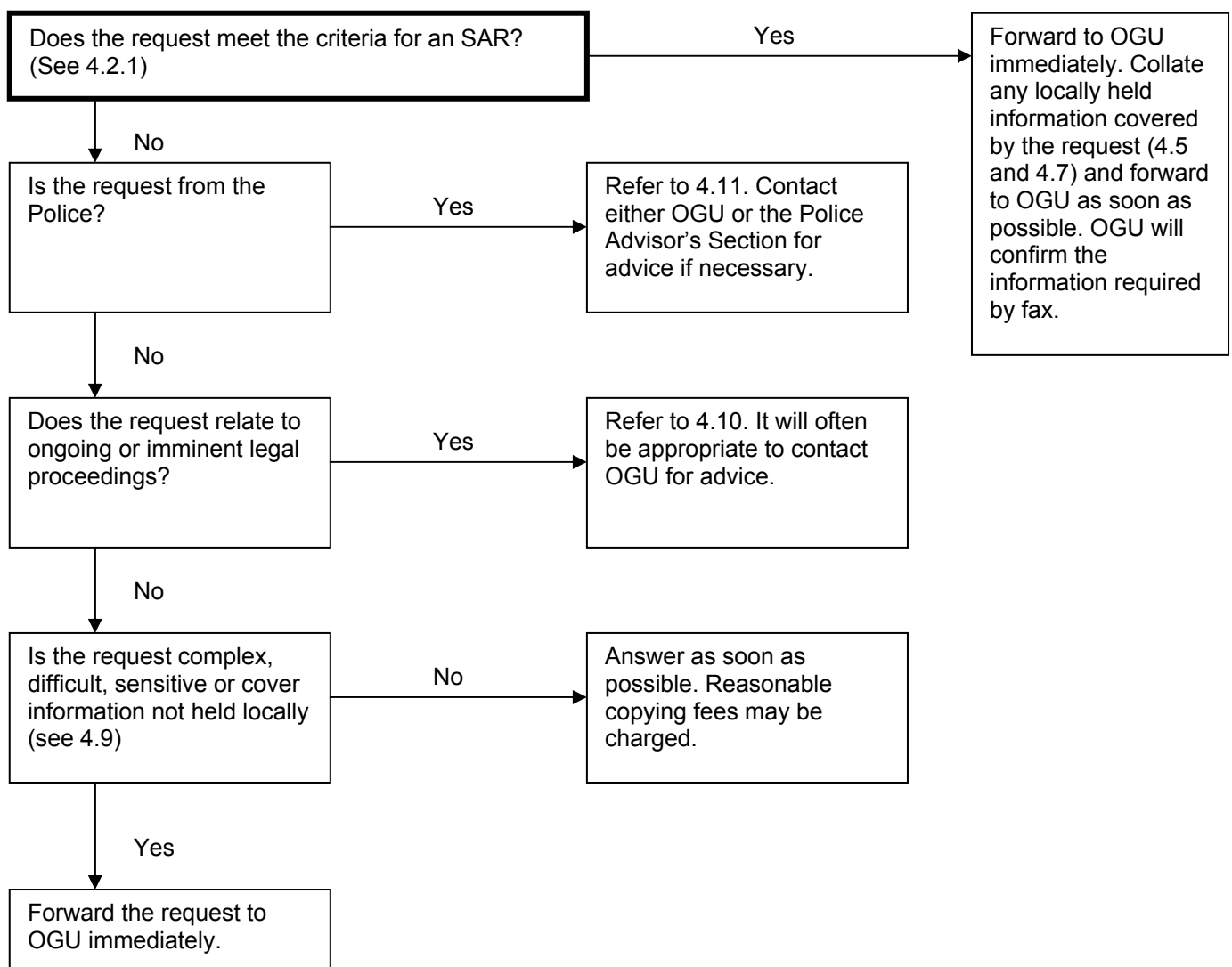
ANNEX B

FLOWCHART: PROCEDURES FOR HANDLING REQUESTS FOR PERSONAL INFORMATION

1. PROCEDURES FOR ALL STAFF



2. PROCEDURES FOR IARs



ANNEX C

FLAGGING AND FEEDBACK PROCEDURES

1. With the exception of security and medical information, it is important that areas/groups do not do their own vetting when handling DPA subject access requests. In the past this has been done by blacking out or otherwise concealing parts of the record. Doing so opens us up to unnecessary legal action or the intervention of the Information Commissioner.

Flagging

2. In the first instance, if there are concerns about a particular disclosure or the DPA in general, contact OGU staff at Branston for advice. (01283 49 60 65 or 49 60 66)

3. The accompanying form can be used to raise any general issues relating to a request for personal data by a particular offender which OGU staff should be aware of when they are vetting it. For example, an offender may have a grudge against a particular member of staff or strongly dispute information on their record to the point where they may assault staff as a result of reading it. The form should form the top-sheet of the offender's information when it is sent to OGU.

4. This procedure is not designed to encourage staff to go through records, looking for issues to flag up. It should be used to highlight issues which are already known.

5. If there are particular entries on a file which it is felt should be removed, please place a numbered post-it note over the entry in question and make a corresponding entry on the bottom half of the flagging form (in the "No." column). This should only be done if the issue can't be covered in the main part of the form. *Please give a reason as to why the entry should be withheld.*

Feedback

6. Staff at Branston will use the right hand side of the form to note what action has been taken in respect of each of the flagging entries.

7. Staff in Branston will bear in mind the flagging issues while vetting. Although they will attempt to accommodate requests to withhold particular entries, this can only be done if the information is covered by an exemption.

8. A copy of the form will be sent to the area when the offender's request is despatched. This is to give staff the opportunity to see if anything they raised concerns about has had to be disclosed. Staff should not amend or delete any material sent by OGU to the offender.

DPA SUBJECT ACCESS REQUESTS: FLAGGING FORM

Name:	DPA Ref:	Are/Unit. Contact:	OGU Contact:
-------	----------	--------------------	--------------

ESTABLISHMENT

BRANSTON

Issue(s) to Be Flagged	Action Taken

SPECIFIC ENTRIES TO BE FLAGGED

No.	Reasons For Concern	Action Taken

Vetted by: **And** **Date:**

ANNEX D

SUBJECT ACCESS REQUEST FORM: STAFF

Complete this form if you would like a copy of the personal data that the National Offender Management Service holds about you. You are entitled to receive this information under the Data Protection Act 1998.

You should send a cheque/postal order for £10 made payable to HM Prison Service.*

We will endeavour to respond promptly and in any event within 40 days of the request being approved i.e. your cheque clearing, if necessary confirmation of identity and any further information required to proceed with your request.

To proceed with your subject access request we require your: -

Full Name:

Your Home Address:

N.B. We will send copies of the information requested to this address unless you state otherwise

Your Date of Birth:

Your DPS / NI Number(s):

Dates of Employment:

A Description of the type of personal data, which you are seeking and the dates for which we should search.

We also reserve the right, in accordance with section 8(2) of the Act, not to provide you with copies of the information requested if to do so would take "disproportionate effort".

If we are not satisfied that you are who you say you are we reserve the right to refuse to grant your request.

If the information you request reveals details, directly or indirectly, about another person we will usually be required to edit them out.

Signed.....

Dated.....

Please return this to:

Open Government Unit
DPA Subject Access Requests
H M Prison Service
Room 410
Abell House
John Islip Street
London
SW1P 4LH

Telephone: 020 7217 2125
Fax: 020 7217 5150

If when you have receive the requested information, you believe that:

The information is inaccurate or out of date; or

We should no longer be holding that information; or

We are using your information for a purpose of which you were unaware; or

We may have passed inaccurate information about you to someone else;

You should notify your local Information Access Representative or relevant department giving your reasons. The information will be reviewed and amended if necessary.