HM PRISON SERVICE

PRISON SERVICE ORDER

Data Protection.

ORDER NUMBER

9020

INTRODUCTION BY THE DIRECTOR

1. This Prison Service Order informs HM Prison Service of guidance on the procedures for dealing with the handling of Prison Service data. It sets out our obligations under the Data Protection Act 1998. In addition it outlines good housekeeping practice with regard to general records management.

Performance Standards

2. This Prison Service Order will partly underpin a Performance Standard on Prisoner and Staff Records and the disclosure of information, which will be issued in the second half of 2001.

Output

3. This PSO provides clear explanations of record management procedures and requests for the disclosure of information.

Implementation

4. This Prison Service Order comes into effect on 24 October 2001.

Impact and Resource Assessment

5. The guidelines largely reflect existing practice in the management of individual records and disclosure of information already established across the estate. However it is clear that record management, disclosure policy and practice is not evenly applied across all establishments and headquarters. This order will promote practice for providing a comprehensive and quick response to requests for access to personal data. The Order should have a positive impact on the efficiency of subject access disclosures and the resolution of complaints and inconsistencies.

   There may be an increase in the number of requests for information but most of the processes will be removed to the Information Management Section (IMS) in Prison Service Headquarters, London. There are no additional monies available to establishments and units, however local discipline offices, personnel departments and other Prison Service units will only be responsible for retrieving and photocopying records and other data when requested to do so by the IMS. It will be the responsibility of the IMS in London to vet data and make decisions on what should and should not be disclosed under the DPA.

   As the response rate to subject access requests made under the DPA is unknown and the procedures in this PSO have not been tested across the estate, a six monthly post implementation review will be made to ascertain what changes may be needed in the future. Any comments or suggested improvements in connection with the PSO would be welcome.

Mandatory Action

6. For governing governors, directors and controllers of contracted-out prisons, heads of groups and units in HQ and central services;

- All staff must have access to and be made aware of their obligations in respect of this order.
- Any application for the release of personal information, from prisoners, staff or the general public and others, must be considered under the terms of the Data Protection Act 1998.
- This Prison Service Order replaces Circular Instruction 23/1990 on Retention of Records.

Audit and Monitoring

7. The mandatory elements of this instruction will be the subject of a compliance audit by the Standards Audit Unit once the Prisoner and Staff Records Standard has been implemented.

Contact

8. Lead Policy Primary contact point: Michael Achow Information Management Section, Room 721 Abell House, John Islip Street. London. SW1P 4LN

Telephone: 020 7217 5915
Fax: 020 7217 5150

NOTE FOR ESTABLISHMENT LIAISON OFFICERS

ELOs must record the receipt of the Prison Service Order – **The Data Protection Act 1998** *their registers as issue* **137** *as set out below. The PSO must be placed with those sets of orders mandatorily required in Chapter 4 of PSO 0001.*

Issue No.	Date	Order No.	Title and / or description	Date Entered in set	ELO Signature
137	11/10/2001	9020	The Data Protection Act 1998		

Clare Pelham
Director of Corporate Affairs

Contents

Annexes

A. Information leaflet "Data Protection Act 1998: Personal Data on Prisoners"
B. Subject Access Request proforma (Prisoner)
C. Subject Access Request proforma (Staff)
D. Request for Inmate Personal Data (General)
E. Request for Inmate Personal Data (Medical Records)
F. Prisoner/Staff Check List
G. Request for Staff Personnel Data
H. Retention Periods for Personnel Documentation
I. Flow Chart Guidance for Discipline/Personnel and other Units

This Prison Service Order must be read in Conjunction with:

PSO 9010	*Information Technology Security Policy*
PSO 1251 / PSI 89/1999	*The Transfer of Public Records from Prisons to Local Record Offices*
CI 21/1992	*Cardphones*
	Prison Service Security Manual

1.0 INTRODUCTION

1.1 The Data Protection Act 1998

1.1.1 On 1 March 2000, the Data Protection Act 1998 (DPA) came into force replacing the Data Protection Act 1984, which only covered personal data held electronically. From 24 October 2001 the Act extends to all personal data in whatever form they are held. The DPA is built around eight 'Principles', which govern how we process personal data and seven 'Rights' for individuals in respect of personal data. The most significant of these is the 'subject access' right which means that we are obliged, on request, to disclose to an individual all the personal data we hold on them, subject to a limited number of exceptions and exemptions (section 4.2) and the payment of a fee (section 4.8)

1.1.2 Failure to meet our DPA obligations may result in an enforcement notice for non-compliance being issued by the Information Commissioner. In addition individuals are entitled to seek compensation for any distress or damage caused as a result of non-compliance of the Act, which may result in legal action against the Prison Service.

1.2 What Are 'Personal' and 'Sensitive Personal' Data ?

1.2.1 'Personal data' means anything that relates to a living, identifiable individual and includes;

- factual information,
- expressions of opinion, and
- indications of intent.
- 'Sensitive personal data' means any information that relates to an individual's;
- ethnic origin
- political opinions
- religious or other beliefs
- trade union membership
- physical or mental health
- sexual life
- offences
- criminal proceedings and sentencing

1.2.3 Therefore the DPA applies to a broad span of the information we currently hold, with the Prison Service holding both personal and sensitive personal data. For a prisoner, this will mean all the 'operational' record, including medical records, CCTV footage, tape recordings and any other data whether they are held manually or electronically. For staff this will mean similar sets of data that are held on personnel files wherever they are located.

1.2.4 The Prison Service assumes control and therefore responsibility for all personal information either generated or obtained from other organizations. As a result it will be the responsibility of the Prison Service to disclose all information that it holds on individuals, whatever the source. This is subject to a limited number of exemptions (section 4.2) and third party consent (section 4.3).

1.3 Principles

1.3.1 The Prison Service has a statutory obligation to process all personal data in accordance with the eight principles of good practice laid down in the Act. 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.

1.4 Rights

1.4.1 All individuals on whom personal data are held enjoy seven statutory rights. 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 (section 1.5.2 and 4.11) to assess if any provision of the Act has been contravened.

1.5 Roles and Responsibilities

1.5.1 Within the Prison Service, the Information Manager is responsible for all Data Protection, Freedom of Information and Records Management issues. The main duties of the Information Manager are to;

- promote good practice within the Prison Service of Data Protection and Information Management issues,
- provide guidance and advice to all individuals be they employed or detained by the Prison Service on their rights and obligations as defined by the DPA,
- enforce the requirements of the DPA consistently and across the Prison Service,
- act as the first point of call for complaints and grievances should an individual feel that the Prison Service has not fulfilled its statutory duty under the DPA,
- raise awareness, and
- act as a first point of contact for members of the public and other organizations.

1.5.2 The Information Commissioner is an independent officer who reports directly to Parliament and provides guidance on general data/information handling practices. The main duties of the Information Commissioner are to;

- promote good practice by organizations in meeting the statutory requirements of the DPA,
- provide information as to an individual's rights under the Act, and investigate complaints, and
- enforce compliance.

1.5.3 The Information Manager and Information Commissioner can be contacted as follows;

	Information Manager	Information Commissioner
	Room 721 Abell House John Islip Street London SW1P 4LH	Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF
Information Line	020 7217 2125	01625 545745
Switchboard		01625 545700
Fax	020 7217 5150	01625 524510
Website	www.hmprisonservice.gov.uk	www.Dataprotection.gov.uk
e-mail	To be arranged	mail@dataprotection.gov.uk

2.0 USING PERSONAL DATA

2.1 'Fit for Purpose'

2.1.1 The DPA states that "information recorded should be adequate, relevant and not excessive for the purposes for which they are processed." This means that the personal data we process should be the minimum necessary to fulfil our current requirements and should not be collected against a possible future need nor retained longer than necessary.

2.1.2 Establishments must provide prisoners and staff, at the beginning of their sentence or employment, with details of how we process their personal data and how they can exercise their subject access rights. A suggested proforma for prisoners can be found at annex A.

2.2 Accuracy, Amendments, and Deletions

2.2.1 All information collected should be accurate and kept up to date. Extra care must be taken to ensure accuracy when transferring information from manual records to computerized and other electronic systems.

2.2.2 There may sometimes be a conflict between the Prison Service and an individual as to the accuracy of information. Where there is a dispute in the accuracy of such information it should be recorded. For example an individual may insist that they are not taking drugs whilst in custody / employment. However there may be some evidence that they are taking drugs. If you simply record that the individual is taking drugs, and it is subsequently disproved, you may be in contravention of the Act. In order to meet the requirements of the Act you should record the offence but also record that the individual disputes the fact. If later it is discovered that the individual is guilty of the offence you may need to modify the original entry to show that your initial assessment was correct. However you might leave the note of the dispute on the record, if it is evidence, that the individual had denied the facts at the time of the original entry.

2.2.3 On receipt of a subject access request the information that is provided must be all that contained in the personal data at the time the request was received.

2.2.4 Changes to data may only be made if they are necessary to correct errors found when complying with the subject access request. On the correction of errors the original and newly corrected data must then be supplied to the individual. When errors come to light, anyone to whom the inaccurate information has been disclosed must be informed of the correction as soon as possible.

2.2.5 Under no circumstances must information be altered in order to make it acceptable to the data subject.

2.3 Consistency

2.3.1 If personal data are stored on a number of systems, e.g. LIDS and the F2508 or PERSONNEL and SPIRE, they must be consistent. This means that the initial recording of information and any subsequent updates must be carried out so that there are no discrepancies wherever the data are held.

2.4 Data Security

2.4.1 Electronic or manual record systems that contain personal data must be operated in such a way as to facilitate retrieval of the information, yet prevent unauthorized access or accidental amendment or deletion of the data. Individuals should also ensure that they minimize accidental loss through theft or negligence and or damage caused by the effects of fire and water.

2.4.2 All record systems containing personal data must be kept in appropriate secure conditions at all times. Manual records, computer printouts etc. must not be left on desks over night and PCs must be logged off when not in use. (PSO 9010 *InformationTechnology Security Policy*)

2.4.3 All data must be stored in secure cabinets/rooms and these should be locked when not in use. Levels of security should be based on the harm that an individual would suffer if their data were disclosed.

2.5 Access

2.5.1 Only authorized staff with a 'need to know' should have access to electronic or manual systems containing personal data.

2.5.2 Live manual records, those relating to current prisoners and members of staff, should be accessible and preferably be located within the same area that they are used.

2.5.3 Dead manual records relating to ex-prisoners and members of staff should be stored where easy access and deposit are possible.

2.5.4 A system must be in place to enable the tracking of all records. This must cover all movements of files and should include prison transfers, court appearances, records removed to wings, staff transfers, requests for dead files from other discipline or personnel departments, etc.

2.6 Storage

2.6.1 Storage locations should be primarily for the use of storing records only. If due to space considerations, other items have to be kept in the same location they must be stored in such a way as not to have the potential of damaging the records.

2.6.2 Records should be stored on shelves in a way that facilitates easy retrieval. This will not only provide for efficient access to the records but will also make checks more effective.

2.6.3 *Dead files on prisoners must be filed alphabetically within destruction date order* (see section 3.3).

2.6.4 Stored records do not need to be boxed unless damage would result otherwise.

2.7 Environmental Factors

2.7.1 Paper records are particularly vulnerable to damage from environmental factors such as fire and water, so storage areas must be selected with this in mind.

2.7.2 Basement areas and attics are particularly susceptible to ingress of water and should be avoided for the storage of records.

2.7.3 Regular checks for the ingress of water should be carried out, including inspection for leaks and dampness.

2.7.4 The layout of storage areas must conform to fire, health and safety and similar regulations.

2.7.5 Smoking must be prohibited in all storage areas.

3.0 RETENTION AND DESTRUCTION

3.0.1 The fifth DPA Principle states that "Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes". Therefore in files and records must be reviewed regularly and destroyed when no longer required. Under the 'subject access' rights we have to, on request, track down and produce all the personal data we hold on an individual, regardless of whether or not we still use it. Finally, there are strong financial reasons not to retain information longer than necessary, as storing records is expensive in staff and accommodation resources.

3.1 Retention Periods

3.1.1

Inmate Medical Records*	All Personal Health Records	10 Years after conclusion of treatment or death.
	Mental Disorder treated under The Mental Health Act 1983	*20 Years after treatment no longer* considered necessary; or 8 years after the patient's death if patient died while still receiving treatment.
	Maternity Records	25 Years.
Inmate Core File and Other Prison Departmental Records**	For Lifers and records selected for special retention (see 3.1.3)	20 Years from date of discharge
	For Prisoners sentenced to a total of more than 3 months in respect of any one period in custody.	6 Years from date of discharge
	For any other prisoner received in to custody (either after sentenced or on remand).	1 Year from date of discharge
Personnel Records	See Annex H for details	

* In accordance with Health Service Circular 1998/217.
** Instructions replace guidelines in Circular Instruction 23/1990.

3.1.2 For prisoner records where a prisoner has entered custody on more that one occasion, the retention period for all back records will be counted from the last discharge from custody, including any previous periods in custody resulted in a longer period of retention. For example, when a prisoner who previously served a sentence of four years has subsequently completed a term of ten months, the retention period will be six years but will now start again from the date of discharge from the 10 month term.

3.1.3 For some prisoner records it may be necessary to retain documents for longer than the recommended period. Prison records selected for special retention will be retained for 20 years or longer in accordance with:

- Instructions issued by the Prison Service, Governor or person acting on the Governor's instructions because information in the records is relevant to litigation, i.e. all records where the former prisoner has sued the Prison Service or individual members of staff or is known to be considering such action, the maintenance of good order or discipline, the interests of justice or the prevention of crime; or

- Instructions given by the medical officer because the prisoner's medical history might make the long-term retention of the record desirable.

Records to be retained in these circumstances should be clearly marked on the outside of the record with the relevant retention instructions.

3.2 Weeding

3.2.1 The weeding of records and files must be carried out on a regular basis. Individual departments should be aware that the regular weeding of files and the destruction of material that is no longer required not only leads to reduced costs and more effective and efficient operations but it is also a requirement of the DPA. It should be noted that only a Qualified Medical Officer or other Health Professional has the authority to weed Medical Records.

3.3 Destruction

3.3.1 Records selected for destruction must be removed in confidential waste bags and should be disposed of by a competent operator.

3.3.2 A Disposal Schedule must be kept of all records sent for destruction. This log should catalogue the prisoners/staff name, prison number/DPS/NI Number, period of time in custody/employment and destruction date and must be kept for a minimum of 20 years after destruction of the original file.

3.4 Records of Historical or Special Interest

3.4.1 Files of historical or special interest should be treated in accordance with PSO 1251 / PSI 89/1999 *The Transfer of Public Records from Prisons to Local Record Offices.*

4.0 SUBJECT ACCESS REQUESTS

4.0.1 An important aspect of the Act is the 'subject access' right. This gives individuals the right, on request and payment of a £10 fee, to be informed whether we process personal data relating to them, what we use it for and to whom we disclose it. We are then obliged to provide a copy of the personal data "in an intelligible form". There are, however, a limited number of exceptions to this right and these are covered in sections 4.2 and 4.3.

4.1 Access to Personal Data

4.1.1 Subject to 4.1.3. below, the Prison Service will not disclose any personal data to a third party unless the full consent of the subject has been given. However there is provision under the Act for disclosure "in order to protect the vital interests of the data subject", for example in life and death situations where an individual is judged incapable of giving informed consent.

4.1.2 The Act allows for information to be disclosed to other parties as part of the routine work of the Prison Service. To do so, disclosure of such information should be necessary, relevant, and essential to the Prison Service's work with individuals and to the proper administration of the Service. Information may be disclosed to parties with whom the Prison Service has an agreed protocol, e.g. Police and Probation Service etc. and to organizations that have a statutory right such as Courts and Inland Revenue etc. Further, information will be disclosed under the direction of a court order.

4.1.3 Positive steps must be taken to ensure confidentiality. It is a criminal offence under the Act to disclose personal data, knowingly or recklessly, outside the terms of the Home Office Notification and individuals can personally be held criminally liable. Therefore it would be clearly inappropriate for a member of staff to divulge personal data on anyone without the proper authority.

4.1.4 Data subjects have redress through the Information Commissioner if their personal data are unjustifiably recorded or disclosed to third parties. Therefore disclosure of any data however insignificant it may seem, for example the acknowledgement that an individual is held in custody or employed by the Prison Service, may be a breach of the Act. The individual or organization making a request for information on prisoners or staff must have written consent from the subject before information can be disclosed unless there is a statutory requirement for disclosure.

4.1.5 The responsibility for confidentiality also extends to personal data held by third party organizations. As such it is an offence to obtain personal information, for instance from a partner organization, which is not relevant to the Prison Service's business.

4.2.1 Exemptions

4.2.2 The right of an individual to a complete copy of their personal data must be respected but there are a limited number of exemptions to this rule. We are not obliged to disclose personal data relating to, for example, national security or what we believe would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. However the fact that a record may contain some exempt items does not mean that we can turn down the entire subject access request: we are obliged to produce as much information as we can, editing the record as necessary.

4.2.2 There are no blanket exemptions on disclosing personal data that the Prison Service holds and as such all subject access requests must be considered on case by case basis.

4.2.3 The Data Protection (Subject Access Modification) (Health) Order 2000 provides an exemption from subject access rights to medical records where permitting access to the data would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person (which may include a health professional). Decisions taken to withhold personal data on these grounds should only be taken by or on the advice of a health professional.

4.2.4 General data/information may be withheld if it would be likely to cause serious harm to the mental or physical condition of the data subject or any other person. See also section 4.7 Medical Records.

4.2.5 Any decision to withhold access to personal data will be taken by the Information Manager, who will consult with our legal advisers and the Information Commissioner if necessary. An exception is disclosure of Security and Intelligence information, see Section 4.6.

4.3 Third Party Information

- Frequently data on records will contain information relating to another individual, perhaps a fellow prisoner, spouse or child. In such cases we are obliged to release the information but we are not required to release anything that identifies the third party unless they have agreed to its disclosure or, in the particular circumstances, it is reasonable to disclose even without that third party's agreement. Note that when information is released with third party names deleted, the records may still contain sufficient information, that, together with data already held or likely to come into the possession of the person making the request, could identify the third party that gave the information originally. In such circumstances the information relating to the third party should also be withheld.

- The Prison Service cannot refuse access to information on the grounds that the identity of a third party would be disclosed in cases where the information is contained in a health record and the third party is a health professional who has compiled or contributed to that health record or has been involved in the care of the data subject in his capacity as a health professional, unless serious harm to that health professional's physical or mental health or condition is likely to be caused by doing so.

4.3.3. The Prison Service will disclose information and assume ownership of information, subject to exemptions (section 4.2), obtained from third parties under agreed protocols and or by secondments to the Prison Service, e.g. police files and probation reports. When disclosing such information it may be advisable to inform the relevant party who was initially responsible for the information, although it will be the decision of the Prison Service on whether the data are disclosed.

4.4 Relevant Filing Systems and Data Structure

4.4.1 In order to meet the requirements of the Data Protection Act Prison Service data should only be released if it is structured and held in or forms part of a 'relevant filing system'. This means that if data held do not form part of such a system or are not structured they need not be considered for disclosure.

4.4.2 Recently obtained legal advice suggests that only "highly structured" files can be said to constitute a "relevant filing system" within the meaning of the DPA. This means that as well as referring to a specific individual or topic, a manual file must have an internal structure that permits easy access to a particular item. For example, a single file on a person, subdivided by topic or a set of records on a particular subject comprising a number of files on individuals would be a "relevant filing system". A single file on an individual containing papers in no particular order or filed chronologically would not.

4.4.3 A record will be considered to be structured if it:-

- Has coloured or coded dividers, such as the yellow F2050, blue F2051 custodial documents file and green F2052 record of events file.
- An index or other device for locating information/data stored within
- Is by its definition based on one subject, e.g. Medical Files, Chaplaincy reports, education records, etc.
- Is a PDP file that is numbered and subdivided

Data considered not to be structured or held in a 'relevant filing system' would most likely be found:-

- in old records without coloured subdividers and indexes.
- in filing systems where no identifying numbers or devices would enable easy retrieval.

However if in doubt on whether a file is structured or not the Information Management Section in Abell House must be consulted for further advice.

4.5 Processing Subject Access Requests

4.5.1 The Information Management Section (IMS) at Prison Service Headquarters in Abell House will be responsible for managing subject access requests.

4.5.2 All subject access requests must be completed within forty days of receipt of the request and or the fee being cleared or receipt of any necessary additional information needed to process the request. It is therefore of the utmost importance that all stages of the process are carried out without delay.

4.5.3 Any subject access requests received by Establishments or Headquarters Departments should be simply acknowledged and then immediately passed to the IMS at Headquarters. The Information Manager will then be the contact throughout the disclosure process and will deal with all banking issues and requests for the transfer of prisoner monies (section 4.8), in addition to seeking further information if needed in order to comply with the subject access request. *Ad hoc* requests for information are dealt with in section 4.10.

4.5.4 A subject access request must be made in writing, by letter, fax or e-mail.

4.5.5 Ideally a subject access request should be made on one of the standard proformas at annexes B and C. These are available upon request from the Prison Library, Discipline/Custody Office, Hospital Administration, Personnel Office or the Information Management Section in Headquarters. However there is no requirement to use these particular forms.

4.5.6 On receiving a subject access request, the Information Manager may request as much additional detail as is reasonably necessary to locate the personal data required or confirm the identity of the person making the request. This may include date of birth, prison/employee number, dates in custody/employment, and signature.

4.5.7 The Information Manager may refuse a subject access request if an identical or similar request has been made in the recent past.

4.5.8 Once the Information Manager is satisfied, he will approach establishments and or Headquarters departments and units using the forms set out in annexes D,E and G.

4.5.9 All the personal data held on a data subject must be disclosed subject to the exemptions set out in section 4.2. Typically the information found may include;

Prisoners	Prison Service staff
• Core File	• Pension and pay details
• Chaplaincy Records	• PPRS
• Education and Training Records	• Reports
• Inmate Medical Record (IMR)	• PACDAPs
• Lifer Files	• Employment Contracts
• Parole Dossier	• Disciplinary Reports
• Physical Education Records	• ASRs
• Policy Files	• Attendance records
• Probation Information / Files	• Promotion / selection board files
• Psychology Reports	• Recruitment information
• Sex Offender Reports	• Establishment personnel files
• Security Records – 2058	• Other Records and Policy Files
• Warrant Details	
• Workshop Records	
• Other Records and Policy Files	

4.5.10 It will be the responsibility of the Discipline Office or the Personnel Department, upon instruction from the Information Manager, to collect all personal data held within relevant departments, see Annex F. Because of the time limits set out by the Act, this information must be collected within ten working days.

4.5.11 Upon request from the Discipline Office it will be the responsibility of individual departments or the establishment/headquarters personnel office to apply the relevant filing system test as outlined in Section 4.4. If these requirements are met departments/units should copy and flag up any information they feel is covered by the exemptions set out in section 4.2, or where they have particular concerns over its disclosure. (If you feel that the requirements in Section 4.4 may not be met, you must consult IMS for guidance).

4.5.12 All information copied should be ordered in such a way that it reflects the construction of the original record/files.

4.5.13 Information should be provided in an "intelligible form". If any information to be released is written in code an explanation or key to the information should be included with the disclosure. If translations or other alternative types of access are required, IMS in Abell House should be notified in order to give further advice on disclosure.

4.5.14 Once copied, prisoner data should be forwarded to the Discipline/Custody Office for onward dispatch to IMS in Abell House by Recorded Delivery, for collation and disclosure to the subject. Staff data should be sealed and forwarded directly from the personnel department to IMS.

4.5.15 Computer printouts of personal data, including anything held on locally developed systems, should be forwarded to Headquarters together with the manual records.

4.5.16 There may be a few occasions where to copy the files held would result in a disproportionate amount of work. If this is the case, the Information Manager in Prison Service Headquarters must be approached in order to give further advice on disclosure.

4.6 Security Records

4.6.1 Because of the nature of the information, special handling arrangements have been introduced for dealing with subject access requests for security and intelligence data. These differ in part from the procedures for handling subject access requests for non-security related personal data as set out in this PSO.

4.6.2 On receipt of a subject access request, IMS will notify the relevant security establishment/department that a request has been made. A deadline for returning the data will be included.

4.6.3 Security departments will then consider the request against the exemptions contained in the DPA and decide whether any of the personal data contained in the record should not be disclosed. If necessary guidance should be sought from the IMS.

4.6.4 On completion of vetting, the information to be disclosed should be copied or if appropriate, summarized and sent under sealed cover directly to IMS in Room 721, Abell House.

4.6.5 IMS will complete the vetting of information, consulting if necessary before making the final disclosure. A copy of all information forwarded for disclosure should be retained for future reference in case of a subsequent request or dispute. If required, copies of disclosed information will be forwarded to the Head of Security at the originating establishment.

4.6.6 Requests for material other than manual records or electronic files, such as CCTV footage and tape recordings must be reported to the Information Manager for further advice.

4.7 Medical Records

4.7.1 Medical data held on individuals is fully disclosable irrespective of whether it is held as part of a relevant filing system. There are, however, some additional exemptions to the general right of access under the Act; these are covered in section 4.2. Issues concerning information contained within an IMR, which may identify, or have been provided by, third parties are covered in section 4.3.

4.7.2 Requests from GPs and NHS agencies for copies of inmate medical records, or information contained therein, should be directed to the Senior Medical Officer or responsible doctor. Such requests should be accompanied by evidence of patient consent to disclosure. No charge should be made for any request of this nature.

4.7.3 All medical records must be sealed and marked 'Medical in Confidence' when they are being transferred within/between establishments or to Prison Service Headquarters and to the subject making the access request.

4.7.4 Employee medical records held by personnel departments may only be released with the authority of the medical practitioner/officer who compiled the original report/record unless disclosure to the subject has already been made.

4.8 Fees

4.8.1 A fee of £10 will be charged for all subject access requests. Payment can be made by either a cheque or postal order made payable to HMPS. For prisoners, the Information Manager will issue a receipt and where necessary, request the relevant discipline office to deduct prisoner monies by the same amount.

4.9 Requests from Solicitors and Legal Representatives

4.9.1 Subject access requests made by solicitors and other legal representatives on behalf of their client should be forwarded to IMS in the normal way.

4.9.2 Other requests from solicitors and legal Representatives will continue to be dealt with locally in line with existing practice. Any queries should be referred to the Information Manager at Abell House.

4.10 *Ad Hoc* Requests

4.10.1 The formal procedures necessary to process subject access requests under DPA should not interfere with the routine exchange of information essential for carrying out day-to-day business. Approaches from prisoners and staff for limited access to their records need not be treated as a full subject access request and should be handled locally. For example;

- a request by a prisoner to view their money account, property card or other particular piece of information.
- information that the prisoner would be expected to see or be an integral part of their period of time in custody, e.g. random drug test results, adjudications, etc.
- requests from staff for pay history details
- copies of PPRRs
- leave sheets, etc.
-
- Discretion should be used when deciding what can be released, if in doubt you should seek advice from the IMS in Abell House.

4.10.2 Any *ad hoc* requests that involve third parties or confidentiality issues should be referred to the Information Manager at Abell House for advice.

4.11 Complaints

4.11.1 An individual may apply to the Information Commissioner or the courts if they feel that the Prison Service has contravened its obligations under the Act. Individuals have the right in certain circumstances to claim compensation for damage and distress caused by a breach of the Act.

4.11.2 Any complaints or indications of possible legal challenges under the Act should be referred to the Information Manager without delay.

ANNEX A

DATA PROTECTION ACT 1998: PERSONAL DATA ON PRISONERS

In order to carry out its work and meet its obligations to the public, the Prison Service is required to record a variety of information on all prisoners.

Starting with basic identifying information, the Prison Service will record information during your time here. This will include medical reports, training records, disciplinary reports and any other relevant information.

We also share information with a number of other agencies such as the Police, Crown Prosecution Service, Courts and Probation Services. All this information is treated in the strictest confidence.

It is your right under the Data Protection Act 1998 to have access to this personal data. To do so you should make an application in writing via the Discipline/Custody Office, Personnel Department or Library. You will need to pay a fee of £10 for access to your records and, for convenience, we would suggest that you make your application on a Subject Access Request form. However any form of written request will be acceptable. We will then let you have a copy of the information required. We are required by law to withhold some types of information, for example where the identity of a third party may be revealed or if the data have been gathered for the prevention and detection of crime.

For further details on the Data Protection Act, you should refer to PSO ##/2001, *The Data Protection Act 1998*, which is held by the Library or Establishment Liaison Officer.

If you have any further enquiries on how the Prison Service uses the personal data we keep on you, please contact;

The Information Manager
H M Prison Service
Room 721
Abell House
John Islip Street
London
SW1P 4LN

ANNEX B

DATA PROTECTION ACT 1998: SUBJECT ACCESS REQUEST (PRISONER)

You should complete this form if you want us to supply you with a copy of personal data, which we hold about you. You are entitled to receive this information under the Data Protection Act 1998.

You should send a cheque/postal order made payable to HM Prison Service, or we will deduct from your prisoner account the sum of £10. (See foot note).

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:

Establishment(s):

Your Date of Birth:

Your Prison Number(s):

Date of Sentence:

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 have to seek the consent of that person before we can let you see that information. In certain circumstances we may not be able to disclose the information to you.

I confirm that I have read and understood the terms of this subject access form.

Signed.....

Dated.....

Please return this form to:

Information Management Section
DPA Subject Access Requests
H M Prison Service
Room 721, Abell House
John Islip Street
London
SW1P 4LN

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 the Discipline Office or relevant Establishment Department at once, giving your reasons. The information will be reviewed and amended if necessary.

Name
Establishment
Prison Number

I authorize the Prison Service Information Management Section to deduct the sum of £10 from my prisoner account no.....

Signed

ANNEX C

DATA PROTECTION ACT 1998: SUBJECT ACCESS REQUEST (STAFF)

We request that you should complete this form if you would like a copy of the personal data that the Prison 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 have to seek the consent of that person before we can let you see that information. In certain circumstances we may not be able to disclose the information to you.

Signed.....

Dated.....

Please return this to:

Information Management Section
DPA Subject Access Requests
H M Prison Service
Room 721, Abell House
John Islip Street
London
SW1P 4LN

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 the Personnel Office or relevant department giving your reasons. The information will be reviewed and amended if necessary.

ANNEX D

DATA PROTECTION ACT 1998: REQUEST FOR INMATE PERSONAL DATA (GENERAL)

The Prison Service has received a request from (*prisoner name*), (*prisoner number*) for the disclosure of personal data held by the department/unit. (*prisoner name*) is currently held / served from (*date*) to (*date*) in your establishment.

Would you please make a copy of the /all records and any other information, manual or electronic, that you hold on this prisoner. You should flag up anything that you feel should not be disclosed with reasons. When you have copied the records, these should be forwarded to the Discipline Office for despatch to IMS in Abell House.

PSO ##/2001, *The Data Protection Act 1998*, contains advice on how to deal with this request but if you have any queries, please contact the Information Manager at the address below.

Information Management Section
DPA Subject Access Requests
H M Prison Service
Room 721
Abell House
John Islip Street
London
SW1P 4LN

Telephone: **020 7217 2125**
Fax: **020 7217 5150**

ANNEX E

DATA PROTECTION ACT 1998: REQUEST FOR PRISONER PERSONAL DATA (INMATE MEDICAL RECORD)

The Prison Service has received a request from (*prisoner name*), (*prisoner number*) for the disclosure of their Inmate Medical Record. (*prisoner name*) is currently held / served from (*date*) to (*date*) in your establishment.

Would you please make a copy of all records and any other information, manual or electronic, that you hold on this prisoner. When you have copied the records, these should be sealed, marked 'Medical in Confidence' and forwarded to the Discipline Office for further action.

PSO ##/2001, *The Data Protection Act 1998*, contains advice on how to deal with this request but if you have any queries, please contact the Information Manager at the address below.

Information Management Section
DPA Subject Access Requests
H M Prison Service
Room 721
Abell House
John Islip Street
London
SW1P 4LN

Telephone: 020 7217 2125
Fax: 020 7217 5150

ANNEX F

PRISONER/STAFF CHECKLIST

Prisoner/Staff Name				
Prison/Employment Number				
Establishment/Unit/Department				
Request Received				
Department	**Request Sent**	**Information Received**	**Information Sent to IMS Abell House**	**Notes**
Inmate Core File 2050 Inmate Medical Record Psychology Reports Physical Education Education Records Workshop Records Chaplaincy Any Other Prison Departments where Records/Information may be held.				

ANNEX G

DATA PROTECTION ACT 1998: REQUEST FOR STAFF PERSONAL DATA (GENERAL)

The Prison Service has received a request from (*staff name*), (*staff number*) for the disclosure of personal data held by your department/unit. (*staff name*) is currently employed / employed from (*date*) to (*date*) in your establishment / department.

Would you please make a copy of /all records and any other information, manual or electronic, that you hold on this member of staff. You should flag up anything that you feel should not be disclosed with reasons. When you have copied the records, these should be forwarded to the Information Manager for action.

PSO ####, *The Data Protection Act 1998*, contains advice on how to deal with this request but if you have any queries, please contact the Information Manager at the address below.

Information Management Section
DPA Subject Access Requests
Room 721
Abell House
John Islip Street
London
SW1P 4LN

Telephone: **020 7217 2125**
Fax: **020 7217 5150**

ANNEX H

Retention Periods for Personnel Documentation

These retention periods have been taken from guidance issued by the Public Record Office and Cabinet Office in DEO(PM) 98/1.
The following list details the key documents only.
Documents bearing on pension entitlement should generally be kept for 72 years from date of birth or 5 years after last action, whichever is later. This is shown in the following table as 'Until age 72'.

Document Description	Retention Period
Employment and Career	
Written particulars of employment, contracts and changes in terms and conditions.	Until age 72
Current address details	6 years after employment has ended
Working time directive opt out forms	3 years after the opt-out has been rescinded or has ceased to apply
Record of previous service dates	Until age 72
Qualifications / references	6 years
Annual / Assessment Reports	5 years
Job applications – internal and recruitment, appointment and / or board selection papers	1 year
Bank and Building Society references	6 months
Health	
Health Declarations, Health referrals, medical reports from doctors and consultants etc.	Until age 72
Medical reports of those exposed to a substance hazardous to health.	50 years from date of last entry
Medical / Self Certificates – unrelated to industrial injury.	4 years
Pay and Pension	
Bank details – current	6 years after employment has ended
Death Benefit Nomination and Revocation Forms	Until age 72
Death, Marriage and Decree Absolutes	Return original to provider. Retain copy until

	age 72
Housing Advances	6 years after repayment
Unpaid leave periods (maternity leave etc)	Until age 72
Maternity documentation	6 years
Payroll history, overtime, allowances, pensions estimates and awards etc.	Until age 72
Names, DoB, NI Number and papers relating to pensions	Until age 72
Resignation, termination and retirement letters	Until age 72
Advances for Season Tickets, Car Parking Bicycles, Christmas / holidays, Housing	6 years after repayment
Personal	
Welfare papers	Destroy after minimum of 6 years after last action.
Security	
Security personnel files	

ANNEX I

Subject Access Request Disclosure of Information
Guidance for Discipline/Personnel Offices and other Prison Service Units