HM PRISON SERVICE

Prison Service Order

ORDER NUMBER

1215

Professional Standards: Preventing and Handling Staff Wrongdoing

Date of Issue / Amendment	Click on Number for link to reference
17/02/2003	
Amendments can be tracked in the Numerical Index.	
PSI Amendments should be read before and in conjunction with PSO	

Order Ref: 1215

INTRODUCTION BY THE DEPUTY DIRECTOR GENERAL

The purpose of this Prison Service Order is to support a culture committed to high personal and professional standards, to set out mandatory requirements and guidance on preventing wrongdoing, supporting vulnerable staff, reporting wrongdoing procedures, processing of information and integrity testing of staff.

Performance Standard

This PSO supports the delivery of the Performance Standards on Conduct and Discipline and the proper delivery of the Security Standard and all standards relating to the treatment of staff and prisoners.

Output

The benefits for the Service from this PSO will be:

- The maintenance of high standards of personal and professional conduct.
- The prevention of some wrongdoing.
- Greater probability that wrongdoing will be reported and addressed.
- Recognition that staff wrongdoing is an issue, and that the Service is committed to dealing with it.
- A properly formulated system for managing information on suspect staff.
- Effective co-ordination between local, Area and Service level action.
- Through the use of integrity testing to check out speculation and to facilitate the satisfactory resolution of cases that would otherwise remain unresolved.

Impact and Resource Assessment

This PSO is likely to require a modest increase in the administrative effort devoted to addressing vulnerabilities and to handling information at establishment and Area level. Area Intelligence Officers are being appointed to support the latter process.

Implementation

This PSO comes into effect on 17 February 2003. Arrangements for compliance should be put in place by 28 March 2003.

Mandatory Action

Mandatory actions are highlighted in italics throughout the text. *Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units must ensure that they are aware of these and must put in place necessary arrangements to deliver these requirements. They must also ensure that all their staff are made aware of any changes in procedure.*

Audit and Monitoring

7. Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units should monitor action in compliance with this PSO as part of routine line management. Oversight of the Service-wide arrangements for dealing with staff suspected of wrongdoing will be provided by a committee chaired by the Director of Personnel. This committee will, among other things, monitor the processes and provide assurance to the Prison Service Management Board that the arrangements are being carried out effectively and with

integrity. Consideration will be given to amending relevant Performance Standards and to the creation of audit baselines relating to the content of this PSO. In the event that baselines are introduced, compliance will be audited by self-audit and by Standards Audit Unit.

Contact

8. Given the nature of the subject this PSO cannot hope to cover all possible eventualities. Advice on this PSO is available from the Head of Professional Standards Unit on 01527 551224. 'Reporting Wrongdoing' calls to PSU should be made on the separate dedicated hotline, the number of which has been publicised - 01527 544777.

Phil Wheatley
Deputy Director General

NOTE FOR ESTABLISHMENT LIAISON OFFICERS
ELOs must record the receipt of this Prison Service Order – 'Professional Standards: Preventing and Handling Wrongdoing by Staff' in their registers as issue 167 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
167	17/02/03	1215	Professional Standards: Preventing and Handling Wrongdoing by Staff		

CONTENTS

CHAPTER 1: INTRODUCTION

1.1 Purpose of PSO

1.1.1 The purpose of this PSO is to support a culture committed to high standards of personal and professional conduct. It sets out mandatory requirements and guidance on preventing wrongdoing, supporting staff who are vulnerable to wrongdoing, reporting suspicions of wrongdoing, on how (prior to a police enquiry or a formal investigation under PSO 1300) information relating to suspected staff wrongdoing must be dealt with and on the use of integrity testing.

1.1.2 The processing of information about staff wrongdoing is to expose and prevent corruption and wrongdoing in the Prison Service

1.1.3 This PSO does not affect the procedures for handling other types of sensitive information.

1.2 Definition of professional standards and staff wrongdoing

1.2.1 The Professional Standards Statement at Annex A is replicated in the 'Standards of Conduct' section of the Code of Conduct and Discipline. It sets out the standards expected of staff in terms of behaviour and describes unacceptable behaviour. For the purpose of this PSO "Staff Wrongdoing" means conduct in breach of the Professional Standards Statement at Annex A of this PSO. This PSO is primarily about actions which may be taken to prevent wrongdoing and the handling of information that indicates or raises the suspicion that a member of staff is in breach of professional standards.

1.3 Arrangements and roles

1.3.1 <u>All Staff</u>

Staff at all levels must demonstrate high standards of personal and professional conduct in accordance with the Professional Standards Statement. Where staff find that they are in a situation where they cannot do so they should deal with this in a responsible way, consulting and advising line managers and others as necessary.

It is also essential that staff report wrongdoing or suspected wrongdoing when they become aware of it. This PSO requires staff to report concerns to local management or to the Professional Standards Unit.

1.3.2 Local management

Local management has a responsibility to create a culture which supports high standards of conduct and in which staff will feel free to:

- be open about vulnerable situations; and
- raise suspicions of others' wrongdoing with their line managers or the designated manager.

Local management must establish arrangements for supporting staff; for the receipt and confidential handling of material; for the evaluation, dissemination and disclosure of the information to others as appropriate. Local management are responsible for handling and dealing with information received. However, local management and Area Managers may wish to involve the PSU and/or Area Intelligence Officers if assistance and support is required, particularly with complex issues and/or when other Areas, establishments or agencies are involved. *Local management must share all information with PSU in order to aid the development and analysis of PSU's Service-wide database.*

It is recognised that HQ Groups and small units (with the possible exception of Area Offices) will not have staff with the expertise or experience to deliver local intelligence handling. Heads of Groups and Units are therefore encouraged to refer cases to PSU for further work on developing intelligence.

1.3.3 Area Management

Area Intelligence Officers (AIO) will be in post to support Area Managers. The role of the AIO will be to assist and support establishments, the Area Manager and the Professional Standards Unit with the development of a wide range of staff related data, information and intelligence, within an allocated geographical area. The AIO will also act as a conduit to assist with the flow of information and intelligence between PSU, Area Office, establishments and other enforcement agencies.

1.3.4 Service-level: the Professional Standards Unit

The Professional Standards Unit has been established to receive, develop and analyse intelligence on wrongdoing in the Service. The PSU will liaise with local and Area level staff and with outside agencies as necessary. The PSU will also receive information direct on the Reporting Wrongdoing hotline (which incorporates the Fraud Helpline).

Information received and developed by PSU will normally be passed to the establishment or Area concerned, and an active role will only be taken when tasked to do so or where the matter is especially complex and involves several establishments.

1.3.5 Investigations

The PSU has also absorbed the Investigations Co-ordination Unit, previously part of the Standards Audit Unit. The Investigation Support Section (ISS) of PSU will provide advice on procedure to investigators, maintain a register of trained investigators, monitor the progress of investigations, maintain statistics, produce reports on investigations and assess the quality of investigation reports and offer advice to the Commissioning Authority.

Investigations will be carried out locally or by Area investigators as decided by Line Management. The PSU is not authorised or resourced to carry out investigations.

Chapter 2: PREVENTION AND SUPPORT TO VULNERABLE STAFF

2.1 Prevention

2.1.1 Our aim is to promote high standards of professional and personal conduct and to prevent wrongdoing. Prevention can be achieved through compliance by staff and managers with Orders and Instructions and by effective and watchful line management. There is also a need to ensure that staff know the standards expected of them, to identify vulnerable systems in terms of policy and procedures and to identify and support staff who may be vulnerable to wrongdoing.

2.1.2 *Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units must ensure that the "Professional Standards Statement" at Annex A is publicised locally.* They are encouraged to make it the subject of staff briefings and discussions and to incorporate it into induction arrangements.

2.1.3 *Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units must review the business of the establishment, Group or Unit with the purpose of identifying processes which may be targeted by, and vulnerable to, those who are involved in wrongdoing.* The annual fraud risk assessment required by PSO 7500 (the Financial Order) is an important tool in identifying vulnerable financial systems. *Consideration must be given to using a similar process to focus on local arrangements for prisoner management and staff administration procedures which might be compromised and leave staff vulnerable to, or able to exploit systems to aid corrupt practices.* At the centre, the Professional Standards Unit will review prisoner management and personnel procedures in consultation with policy leads and will produce reports to help local management identify and deal with risk.

2.1.4 *Where vulnerable systems or situations are identified, they must be removed or reduced.* In some cases it may not be possible to change a procedure, but some wrongdoing may be prevented if staff are aware and expect line management checks.

2.2. Vulnerable staff

2.2.1 *Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units must promote a culture in which staff who may be vulnerable to wrongdoing are encouraged to*

come forward and in the first instance raise the matter with their line manager when appropriate. The Professional Standards Unit will produce publicity aimed at encouraging such staff to discuss their concerns with line managers. Other staff who are aware that a colleague may be vulnerable should also be encouraged to come forward. Vulnerability to wrongdoing may arise through pressure or manipulation by other staff, prisoners, others, or from personal circumstances which may make a member of staff open to financial or other pressures and inducements. *All staff must be made aware of the support available to them through the Staff Care and Welfare Service, Trade Unions, and other organisations both within the Prison Service and outside, and should not be stigmatised for approaching management with their concerns.*

2.2.2 *Staff who have been approached by colleagues, or others, to engage in wrongdoing must report this in line with Chapter 3 of this PSO and the information must be processed in accordance with Annex B to this PSO. Staff must be assured that they will be protected as necessary and may seek confidentiality*, although the nature of the case and the role the individual has played up to the point of coming forward may still lead to disciplinary action being taken against them.

Chapter 3: REPORTING WRONGDOING

3.1 Staff responsibilities

3.1.1 *All staff working in the Prison Service must report wrongdoing by others in the Service that they either witness or become aware of.* Failure to report wrongdoing by others may itself be a disciplinary offence – see the PSO on Conduct and Discipline*. Staff must pass on such information or suspicions to their line management, to the designated manager or to the Professional Standards Unit either via the PSU's Reporting Wrongdoing hotline – 01527 544777 - or the PSU's confidential address – HM Prison Service, PO Box No. 10656, Redditch, B97 6ZU.* Staff are encouraged to disclose their names whenever possible, to ensure that proper verification and evaluation of the information takes place and that it can more easily be acted upon. Anonymous reporters do not discharge their responsibility to report wrongdoing under this PSO.

3.1.2 Staff should use an Information Report for reporting their concerns (the Security Information Report SIR can be used for this purpose).

3.2 Reporting systems and culture

3.2.1 If a culture which challenges wrongdoing is to be developed among staff in the Service it is important that staff and visitors feel free to, and are encouraged to, report wrongdoing. *Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units must:*

i) designate and appoint a manager – 'the designated manager' - as the person who will receive and manage information on wrongdoing;
ii) ensure that staff know who the designated manager is;
iii) ensure that staff are asked to report wrongdoing to their appropriate line manager or to the designated manager, and are reminded of this at least annually;
iv) ensure that forms for reporting wrongdoing are made available;
v) ensure that staff and visitors are made aware of the Service-wide Reporting Wrongdoing hotline located at the Professional Standards Unit;
vi) ensure that the system is operated with integrity; and
vii) promote a culture which encourages the challenging and reporting of wrongdoing.

3.2.2 *The designated manager must report to the Governing Governor, Controller, Director of a privately run prison, Area Manager or Head of*

Group or Unit in respect of activities carried out in compliance with this PSO. If he or she is line managed on other duties by another person, the different lines of reporting and accountability must be clearly set out and understood by all parties.

3.2.3 *The role of the designated manager must be reflected in his or her SPDR.* In selecting the designated manager, account should be taken of the need for the individual to be completely trustworthy, respected and experienced. The designated manager should be someone that staff are likely to feel confident in disclosing information to, when discretion is needed. While not essential, it may be helpful if the person selected for this role in establishments is also responsible for the handling of prisoner intelligence.

3.3. Reporting Wrongdoing hotline

3.3.1 A reporting wrongdoing hotline has been established within the Professional Standards Unit. This is where staff can report any wrongdoing they witness, become aware of or suspect. The Reporting Wrongdoing hotline incorporates the Fraud Helpline run by the Fraud Investigation Unit of Internal Audit. The number is **01527 544777**. Agreed protocols for the exchange of information (fraud related) have been established between the Head of PSU and the Head of Internal Audit.

3.3.2 Calls to the Reporting Wrongdoing hotline will be answered by staff of the PSU. Outside office hours an answering machine will be in operation. All calls will be treated as confidential, logged, and the information received will be evaluated and processed in accordance with the principles laid out in Annex B of this PSO.

3.3.3 Staff and others who call the Reporting Wrongdoing hotline and who disclose their names to PSU may ask for wider confidentiality; i.e. that others including the subject of their suspicions should not know that they made the report. In such cases PSU will comply with such a request; *however the source must be advised that the confidentiality of any information will be protected so far as reasonably possible;* but this may not be possible if it later conflicts with a countervailing public interest, e.g. the prevention or prosecution of serious crime or if disclosure is required by statute or is ordered by a court.

3.4 Confidential written reports

3.4.1 Staff or others who wish to report wrongdoing or suspected wrongdoing may write confidentially to line management, to the local designated manager, to the AIO or to the Professional Standards Unit's confidential

address – HM Prison Service, PO Box No. 10656, Redditch, B97 6ZU. Reports or letters received by line managers should copied to the designated manager and/or to PSU.

3.5 Protection for those making reports

3.5.1 Staff who report wrongdoing should be supported and *must be protected, provided that the report is raised in good faith and that there is a reasonable belief on the part of the member of staff making the report that the information is true.* Victimisation and bullying are disciplinary offences. *Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units must ensure that line managers of staff who are known to have made reports on colleagues are aware of the need to treat subsequent victimisation seriously. If a member of staff reports that he or she is being victimised for making a report the matter must be investigated and a risk assessment carried out to identify the level of risk to the member of staff. Appropriate action must then be taken to protect the member of staff against further victimisation.*

3.5.2 The act of victimisation may itself be useful intelligence and staff who are victimised because of making a report are encouraged to inform the designated manager, especially if there has been no resolution to the case initially reported.

3.6 Malicious or mischievous allegations

3.6.1 The process of evaluation and intelligence development set out in Annex B will minimise the likelihood that malicious or mischievous allegations will lead to unjustified investigations being initiated.

Chapter 4: Managing Information – The Process

4.1 Introduction

4.1.1 The process and procedures for managing information on staff wrongdoing are described at Annex B *and must be followed.* For ease of reference the annex has a separate contents page.

Chapter 5: Integrity Testing

5.1 Introduction

5.1.1 When information is processed indicating that a member of staff may be involved in wrongdoing and the case cannot be resolved by other means, then a test of the member of staff's integrity may be carried out.

5.1.2 **An integrity test may only be used to follow up information that has been processed in accordance with Annex B of this PSO.**

5.1.3 An integrity test is a situation created which presents the suspected member of staff with an opportunity to carry out the alleged wrongdoing*. The use of an integrity test must be a necessary and proportionate response to the suspected wrongdoing.*

5.1.4 The procedures for integrity testing are described at Annex E and must be followed.

Annex A

The Professional Standards Statement

Purpose

Prison Service staff are expected to meet high standards of professional and personal conduct in order to deliver the Prison Service Vision. All staff are personally responsible for their conduct. Misconduct will not be tolerated and failure to comply with these standards can lead to action which may result in dismissal from the Service.

This document therefore identifies and clarifies the key standards of professional and personal conduct expected of all staff.

It should be noted that this is not an exhaustive list. Any conduct that could undermine the work of the Service is not acceptable.

Prison Service Principles

The Prison Service Principles underpin the work of the Service and all staff are expected to act in accordance with them. Staff must therefore:

1. Deal fairly, openly and humanely with prisoners and all others who come into contact with them.

2. Encourage prisoners to address offending behaviour and respect others.

3. Value and support each other's contribution.

4. Promote equality of opportunity for all and combat discrimination wherever it occurs.

5. Work constructively with criminal justice agencies and other organisations.

6. Obtain best value from the resources available.

Conduct Expected

The following sets out the professional and personal standards of conduct expected of all staff.

General

Staff must carry out their duties loyally, conscientiously, honestly and with integrity. They must take responsibility and be accountable for their actions.

Staff must be courteous, reasonable and fair in their dealings with all prisoners, colleagues and members of the public. They must treat people with decency and respect.

All staff must comply with Service policies and procedures. Managers must ensure that standards of behaviour and conduct are maintained.

Discrimination, Harassment, Victimisation and Bullying

Behaviour of this kind is not acceptable and will not be tolerated. Staff must not:

- Discriminate unlawfully against individuals or groups of individuals because of their gender, racial group, sexual orientation, disability, religion, age or any other irrelevant factor.

- Harass others through behaviour, language and other unnecessary and uninvited actions.

- Victimise or bully others through their actions and behaviour.

Further explanation of what is expected of staff in this area is contained in PSO 8010 and the Director General's letter to staff of 11 May 2001.

Relationships with prisoners

Staff must exercise particular care to ensure that their dealings with prisoners, former prisoners and their friends and relations are not open to abuse, misrepresentation or exploitation on either side. Staff relationships with prisoners must be professional. In particular staff must not:

- Provoke, use unnecessary or unlawful force or assault a prisoner.

- Use offensive language to a prisoner.

- Have any sexual involvement with a prisoner.

- Give prisoners or ex-prisoners personal or other information about staff, prisoners or their friends and relatives which is held in confidence.

- Have any contact in or outside work with prisoners or ex-prisoners that is not authorised.

- Accept any approaches by prisoners for unauthorised information or favours and must report any such incidents.

Corruption

Corrupt behaviour is not acceptable. Staff must not solicit or accept any advantage, reward or preferential treatment for themselves or others by abusing or misusing their power and authority.

Conflicts of Interest

Staff must not have private interests that interfere or could interfere with the proper discharge of their duties. This includes financial and business interests but also any personal relationships which could compromise or be perceived to compromise them in the discharge of their duties. Staff must bring any potential conflicts of interests to the attention of a Senior Manager. Governors and Heads of Groups should maintain a register of conflicts of interest for their staff.

Criminal Activity

Staff must not be involved in any criminal activity. They must inform the Governor or Head of Group as soon as possible if they are charged with or convicted (including a police caution) of any criminal offence.

Use of Information

Staff must protect any information which they have obtained through their work in the Service.

Personal Finances

Staff must conduct their financial affairs in a proper and responsible way. If difficulties occur they must inform their manager. The Staff Care and Welfare Service and a “Debtline” are available to staff for advice and support.

Conduct that affects the Performance of Duties

Staff must not take any action on or off duty that could affect, cast doubt on or conflict with the performance of their official duties. For example, outside activities or membership of organisations which promote racism.

Discredit on the Service

Staff must not bring discredit on the Prison Service through their conduct on or off duty.

Civil Service Requirements

Staff must behave with discretion in matters of public and political controversy. They must observe the Civil Service-wide rules relating to political activities and the acceptance of outside appointments.

Staff Responsibility

All staff are personally responsible for ensuring their conduct is in line with the above standards. If staff are in any doubt as to what is acceptable conduct they must seek advice from their line manager.

Staff must challenge and report any possible suspicion of misconduct to their manager. If they are not able to do this they must report it to the Service's Reporting Wrongdoing hotline.

Issues of Conscience

If staff feel that to act or abstain from acting in a particular way would raise for them a fundamental issue of conscience and the problem cannot be resolved by any other means, they may take up the matter with the Director General. If the matter still cannot be resolved on a basis which the member of staff is able to accept, they must either carry out the instruction or resign.

Supporting Documents

This document underpins and complements other Service documents which staff should refer to for further information. These include:

The Staff Handbook
The Code of Conduct and Discipline
PSO 8010 Equal Opportunities for Staff
Director General's letter to staff of 11 May 2002.

Annex B

Managing Information – The Process

B1 General Principles

B2 Standard Grounds

B3 Recording and Retention

B4 Evaluation of Information

B5 Protective Marking

B6 Notifying PSU

B7 Progressing the Case

B8 Sharing/Dissemination of Information

B9 Review, Retention and Destruction of Intelligence Records

B10 Requests for Access to Records

Managing Information – The Process

B1 General Principles

Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units must ensure that procedures are in place locally to deliver these requirements. Area Managers and Heads of Groups and Units must decide the extent to which the requirements will be delivered locally by the 'designated manager'.

Area Intelligence Officers and PSU staff must comply with the mandatory actions for designated managers set out in this PSO, when they are filling the designated manager's role.

Any information on staff wrongdoing received by the designated manager or PSU must be:

i) checked for Standard Grounds;
ii) recorded and stored, and an intelligence record created;
iii) evaluated;
iv) protectively marked, if appropriate;
v) used and developed into intelligence if appropriate;
vi) disseminated or shared, as appropriate; and
vii) reviewed regularly for retention or destruction.

Throughout the processes set out above legal requirements must be met. The creation of an intelligence record must be for a legal purpose. Its development must be necessary and must be a proportionate response to the aim in the context of the specific concerns raised by the information. The dissemination of intelligence must be properly risk assessed and storage of information must comply with the terms of the Data Protection Act 1998.

B2 Standard Grounds

Prison Service staff may record and disseminate intelligence material without the necessity to seek higher level prior authorisation if:

- It is believed that the recording/dissemination of intelligence material is likely to be of value in the interests of national security, the prevention or detection of crime or disorder, the maintenance of community safety, the assessment or collection of any tax or duty or of any imposition of a similar nature, or otherwise serves a significant public interest.

- The recording and dissemination of intelligence material does not include 'confidential material' (see Annex D), unless the specific safeguards have been taken in to account.

- The recording and dissemination of intelligence material would be in compliance with the DPA 1998 (see Annex D).

These are the 'Standard Grounds' and have to be met before the designated manager can legitimately create and retain an intelligence record. The term 'Standard Grounds' is widely used as a convenient shorthand expression for explaining the legal requirements necessary for the gathering and processing of information on staff and others. It is introduced in this PSO for those purposes.

The legal framework at Annex D sets out all of the legislation relevant to the processes to be described and explains in more detail the authority to hold, process and act on intelligence.

B3 Recording and Retention

Staff should report information using the Information Report. The existing Security Intelligence Report can be used for this purpose.

When the designated manager is content that the Standard Grounds are met and it is decided to retain an Information Report, an appropriate date for a retention/destruction review must be set. The date should normally be no more than 12 months from the date of receipt of the information.

Information Reports must be allocated a unique reference number and stored sequentially.

The designated manager must create a formal 'Information Report Register' and record the receipt of information; the date; source if known; and subject's name, but no information on the content. A list of contents for the Register is at Annex C. The 'Information Report Register' must be given a CONFIDENTIAL protective marking and locked in special security furniture – see B5 below.

A report from a source who seeks confidentiality (i.e. whose name is to be known only to the designated manager) must be registered on a separate Confidential Source Register. A model for such a register is at Annex C and further guidance on its use can be obtained from the PSU.

Information about suspected staff wrongdoing must be handled and disseminated with discretion at all times and conform with 'need to know' principles.

B4 Evaluation of Information

The designated manager must evaluate the information recorded on the Information Report using the 5x5x5 evaluation system or the 4x4 system in establishments where the 5x5x5 system is not yet in use. Guidance on how to use the 5x5x5 evaluation system is set out the Security Manual.

B5 Protective Marking

Information reports or other documents must be protectively marked, stored and transmitted in accordance with PSO 9020 and HON 93/1994.

B6 Notifying PSU

All Information Reports must be copied to the Professional Standards Unit. This is to enable a service-wide picture of the nature and extent of corruption and wrongdoing and to identify any trends or themes, that otherwise would not be identified with each area acting in isolation. It is for the designated manager to decide at what stage in the process they wish to do this, and this decision will be based on the nature and contents of the Information Report.

B7 Progressing the Case

There must be a formal tasking procedure which is to decide:

i) whether action should be taken;
ii) what that action should be; and
iii) and by whom is should be taken.

The tasking procedure should be undertaken by the designated manager and the person to whom he/she reports for the purpose of this PSO. This process gives authority to develop the intelligence and gather more information.

The designated manager and/or the person to whom he or she reports must give consideration to whether the intelligence development should be handled locally by the designated manager, at Area level by the Area Intelligence Officer or centrally by or in conjunction with the Professional Standards Unit. If information relates to staff at another establishment, Group or Unit it must not be passed direct to the local designated manager, but must be referred to the AIO for the establishment concerned or to PSU, who must decide whether to pass it down to local level or not. The decision on who should lead on intelligence development will depend on the nature of the information, its implications and any constraints on handling. If it is decided that the case should be handled by others this should be recorded on the Information Report Register and the intelligence record passed on.

A case received from another designated manager, AIO or PSU must be treated as a new report by the receiver. The receiving designated manager must record and protectively mark it as set out in section B5 above. The evaluation codes (apart from the handling code) should not be changed from the original.

There are many different ways in which intelligence can be developed and the handling of each case will depend on the nature and amount of information available. Consideration may be given to the use of Integrity Testing – see Chapter 5 and Annex E of this PSO. If it is decided to employ a covert human intelligence source (CHIS) to develop further intelligence on the case/subject, the principles and systems set out in the Security Manual, in relation to CHIS must be adhered to.

The process of intelligence development must comply with the legal requirements set out at Annex D.

When the intelligence development is complete an intelligence package is created, risk assessed and passed on for action. This action might be the initiation of an investigation. PSU should be informed of the outcome to help with producing a strategic overview for the service.

B8 Sharing/dissemination of information

Intelligence material must only be disseminated or shared on a need to know basis and the risks to the subject, source or third parties must be assessed prior to any dissemination.

The model risk assessment form at Annex C should be followed for a written record of the reasoning process to be made.

If the information received relates to criminal or national security matters it must be referred to the PSU.

B9 Review, retention and destruction of intelligence records

The Data Protection Act 1998 requires that the personal data held on an individual is fit for purpose, accurate, up to date, adequate, relevant, and not excessive for the purpose for which it is held. Such information must only be kept if there is a clear operational need and access restricted to those who are entitled to handle it. Personal data must not be retained for longer than is necessary and periodic review is required. Further guidance on the requirements of the DPA is set out in PSO 9020.

When it is decided to retain an Information Report the designated manager must set an appropriate date for review. The date should normally be no more than 12 months from the date of receipt of the information. At each review the

designated manager must set a new review date if it is decided to retain information. The review dates and confirmation that a review has taken place must be recorded on the Information Report Register. Comments on the review and the reasons for the decision either to destroy the information or to continue to retain it must be recorded on the Intelligence Record.

Documents for destruction must be destroyed in compliance with instructions in HON 43/1994. Confirmation of the date of destruction must be recorded on the Information Report Register.

B10 Requests for access to records

The Data Protection Act gives individuals a right to ask for details of records held on them; including records held for intelligence or security purposes on payment of a £10 fee. Requests for access are managed by Information Management Section. Requests should be dealt with in accordance with PSO 9020 Data Protection.

Annex C

Example Forms

This Annex provides example forms for local use, and a list of data which it is suggested should be included in the Information Report Register.

1 **Information Report Register** – for use by the designated manager.

2 **Confidential Source Register** – for use by the designated manager.

3 **Authorisation and Risk Assessment for Disclosure of Information** – for use by the designated manager, in conjunction with the person to whom he or she reports for the purpose of this PSO.

Information Report Register

The PSO identifies information to be recorded in the Information Report Register. For convenience guidance on the information to be included is listed here:

Establishment/ Group/Unit

Name of Designated Manager

Reference Number of the Information Report

Date the Information Report was received

Who received it

The source of the information report (or a code if source is to be kept confidential)

Evaluation codes of the information report

Reference of Intelligence Record, if created

Review dates

Destruction date

Date and destination of transfer of file to another designated manager etc..

Confidential Source Register

Reference No.	Information Report Reference Number	Date and Time	Source	Remarks	Recording Officer
CSR/SM/001	SLC001	01/06/02 13:00HRS	A N Other A wing	Drugs	[Designated Manager]

Serial Number	**DIS/ /**

RESTRICTEDD

[Click here for printable copy of form]

Authorisation and Risk Assessment for Disclosure of Information

Name	Rank or Grade	Establishment

Description of item for disclosure:

Reason for disclosure:

What is the current handling code? (Circle)

1	2	3	4	5
May be disseminated to other law enforcement and prosecuting agencies, including law enforcement agencies within the EEA and EU compatible (no special conditions)	May be disseminated to UK non prosecuting parties (authorisation and records needed)	May be disseminated to non EEA law enforcement agencies (special conditions apply)	May be disseminated within the receiving agency only	No further dissemination: refer to the originator. Special handling requirements imposed by the officer who authorised collection.

Agency for dissemination:	Disclose / Do not disclose Name……

Does the potential dissemination of the information comply with Standard Grounds?:-

- It is believed that the dissemination of intelligence material is likely to be of value in the interests of National Security, the prevention or detection of crime and disorder, the maintenance of community safety, the assessment or collection of any tax or duty or of any imposition of a similar nature, or otherwise serves a significant public interest.

- The dissemination of intelligence material does not include “Confidential material” as defined unless specific safeguards have been taken into account. An example may be witness or victim reports

- The dissemination of information will be in compliance with the Data Protection Act.
    - Processed fairly and lawfully
    - Obtained for a specific purpose
    - Adequate, relevant and not excessive
    - Accurate and kept up to date
    - Kept for no longer than necessary for the stated purpose
    - Processed according to the rights of the data subject
    - Appropriate organisational and technical security measures
    - Not transferred outside EEA

Has the officer who authorised collection imposed any special handling requirements?

If “Yes” then that officer should be consulted before proceeding with the risk assessment.

Does the material contain confidential or sensitive information?

If “Yes” are there any restrictions on use, or requirements for special handling of the information?

What is the purpose of dissemination?

Are there any ethical, personal or operational risks that are likely as a consequence of disseminating the information?
(The test of proportionality requires assessment of both the character and standing of the subject and the likely consequences to that individual arising from the passage of the intelligence, given the nature and seriousness of the crime subject of the intelligence.)

Having identified any risks, detail the plan to manage them (Consider PII if applicable)

1 May be disseminated to other law enforcement and prosecuting agencies, including law enforcement agencies within the EEA and EU compatible (no special conditions)	**2** May be disseminated to UK non prosecuting parties (authorisation and records needed)	**3** May be disseminated to non EEA law enforcement agencies (special conditions apply)	**4** May be disseminated within the receiving agency only	**5** No further dissemination: refer to the originator. Special handling requirements imposed by the officer who authorised collection.

Following this risk assessment, what is the revised handling code? (Circle)

Disclosed by …… Rank …….
Date …….

Signature ……...

Received by …….. Rank …….
Date ……..

Signature

Record details in dissemination register

Keep in dissemination file

Annex D: The Legal Framework

The action of creating any intelligence record must be justified and properly controlled. The relevant legal provisions are:

- the Data Protection Act 1998 (Prison Service Order 9020);
- the Human Rights Act 1998; and
- the Regulation of Investigatory Powers Act 2000.

These must be adhered to on all occasions to ensure that information is being handled and processed legally and fairly.

The Data Protection Act

The processing (which includes collection, retention and disclosure) of any intelligence or information on any individual is likely to require adherence to the Data Protection Act 1998. This Act requires such data to be processed in accordance with eight principles, which are that the data must be:

- Processed fairly and lawfully
- Obtained for specific purpose
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Kept for no longer than is necessary for stated purpose
- Processed according to the rights of the data subject
- Subject to appropriate organisational and technical security measures (against theft, loss, damage or misuse)
- Not transferred outside the European Economic Area.

As part of the requirement to process data "fairly and lawfully", specific conditions set out in Schedule 2 to the 1998 Act must be complied with, together with additional conditions required for processing any "sensitive" personal data (e.g. details about sex life, possible commission of criminal offences, health etc.). There are exemptions from the need to comply with all aspects of these eight principles in certain circumstances, e.g. where necessary to prevent and detect crime.

The Human Rights Act 1998/ European Convention on Human Rights

The Human Rights Act 1998 made the European Convention on Human Rights (ECHR) part of UK law from 2 October 2000. Particularly relevant to the management of staff-sensitive information is Article 8, the 'right to respect for his private and family life, his home and his correspondence'.

This is qualified by Article 8 (2), which states:

> 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

Any intrusions into a person's privacy must be justified with reference to Article 8 (2). In addition, the principle of proportionality requires that any intrusion must be the minimum necessary to protect 'public safety, or the economic well-being of the country, for the prevention of disorder…' In other words, proportionality dictates that you must not use a sledgehammer to crack a nut.
This article impacts on a vast range of issues and subjects, including:

- Interception of correspondence
- Telephone tapping and search warrants (at home or work)
- Access to information about a person's own identity
- Freedom to express one's sexuality
- Collection and use of information concerning an individual
- The right to have and form social relationships
- Protection of a person's reputation.

The Regulation of Investigatory Powers Act (RIPA)

RIPA is the legislation that provides designated public authorities with the authority to use certain investigatory powers which would otherwise contravene human rights legislation. We can make use of most of the investigatory powers covered by the Act:

- The interception of communications
- Intrusive surveillance, described as covert surveillance, which takes place on residential premises
- Directed surveillance – covert surveillance in the course of specific operations
- The use of Covert Human Intelligence Sources

However, there are two RIPA investigatory powers available to police, but not to us:

- The acquisition of communications data (basically it covers, for example, finding out billing data if you find a mobile phone in your prison and you want to know what numbers have been called)

- Gaining access to encrypted data.

If RIPA applies, the level of authority shown below must be obtained before an activity can be undertaken against a member of staff:

Type of Activity	Authorisation Level
Intrusive surveillance	Secretary of State
Directed surveillance	Area Manager or equivalent
Use of sensitive source *	Area Manager or equivalent
Use of other source	The person to whom the designated manager reports on the specific case under this PSO
Interception of communication	The person to whom the designated manager reports on the specific case under this PSO
When confidential material is likely to be obtained	Deputy Director General

* This covers under 18's, vulnerable prisoners, prisoners being used to participate in specific incidents or threats.

Annex E: Integrity Testing

Procedures

A decision to carry out an integrity test must be taken by the person to whom the designated manager reports for the purpose of the case under this PSO – i.e. the Governing Governor, Controller, Director of privately run prison, Area Manager or Head of Group or Unit.

When a decision to carry out an integrity test is made the name of the authorising officer and the date must be recorded on the intelligence record. The reason for the decision to carry out a test, and reasons why other action, such as a formal investigation under PSO 1300 or a simple enquiry, is considered inappropriate, must also be recorded.

It is essential that the arrangements for integrity testing meet obligations under the Human Rights Act and the Regulation of Investigatory Powers Act. Designated managers and Governing Governors, Controllers, Directors of privately run prisons, Area Managers and Heads of Groups and Units **must take advice from the Professional Standards Unit before engaging in integrity testing for the first time**. The Professional Standards Unit will be able to offer advice on the methods which can be adopted for integrity testing and their legality. Good practice from sources within the Service and from outside agencies will be collated and available for dissemination, thus helping us to avoid the pitfalls such as 'entrapment', which can render evidence obtained inadmissible.

Following a test the case must be reviewed by the authorising officer and the designated manager. The outcome of the integrity test must be recorded in the intelligence record. In many cases where the subject fails the test there will immediately be sufficient evidence for a formal disciplinary investigation to be initiated. This must be proceeded with in accordance with PSO 1300. A statement on the integrity test may be needed for the disciplinary process.

In cases where the subject passes the test the intelligence assessment must be reconsidered and a new decision made on whether there is cause to continue with the case. There is no bar to further integrity tests being carried out but justification must be established and the test must still be necessary and proportionate.

Designated managers must report cases of the use of integrity testing and the outcome of action to PSU to enable good practice and problems to be collated

and shared. This can be done without divulging any details/names that should not be disclosed.