Ombwdsmon
Ombudsman
OMBWDSMON GWASANAETHAU CYHOEDDUS CYMRU
PUBLIC SERVICES OMBUDSMAN FOR WALES

Information Security Policy

Information Security Policy

Contents

Information Security Policy

1 Purpose

1.1. The Public Services Ombudsman for Wales (PSOW) is a public body, with information processing as a fundamental part of its function. It is important that we have a clear and relevant Information Security Policy. This is essential to our compliance with data protection and other legislation and in respecting confidentiality of the information entrusted to us.

1.2. The purpose of this policy is to protect, to a consistently high standard, all information assets. The policy covers security applied through technical and organisational measures as well as the behaviours of people managing the information in line with our business processes.

1.3. This policy is a key component of the Ombudsman's overall information security management framework and should be considered alongside other PSOW documentation including:

- Business Continuity Contingency plan
- Staff Standards of Conduct
- Risk Register
- Freedom of information/Data Protection Policy
- Confidential disclosure (Whistle-blowing)

2 Aims

2.1 The aims of the PSOW's Information Security Policy are to preserve:

- **Confidentiality** - Access to data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.
- **Resilience** – systems shall continue to operate under adverse conditions and be restored to an effective state.

3 Objectives

3.1 The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks (information assets) owned or held by PSOW by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for information security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation, including working collaboratively with suppliers over developing and maintaining secure systems and processes.
- Creating a climate which encourages the reporting of breaches of this policy.

4 Scope

4.1 This policy relates to all information, information systems, networks, applications, locations and users of the Ombudsman's services or supplied under contract to it.

4.2 The policy applies to all PSOW staff (including permanent staff, contract staff, temporary staff) and individuals or organisations contracted directly by PSOW).

5 Definitions

PSOW	The Public Services Ombudsman for Wales
COODOI	The Chief Operating Officer and Director of Improvement
ITM	Information Technology (IT) Manager
CLADOI	Chief Legal Adviser and Director of Investigations (also SIRO)
SIRO	Senior Information Risk Owner
IGM	Information Governance Manager
Personal data	as defined at Article 4(1) of the General Data Protection Regulation (GDPR) as follows: "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"
Special categories of data	As defined at Article 9(1) of the GDPR
	• racial or ethnic origin;
	• political opinions;
	• religious or philosophical beliefs;
	• trade union membership;
	• genetic data;
	• biometric data for the purpose of uniquely identifying a natural person;
	• data concerning health; and,
	• data concerning a natural person's sex life or sexual orientation.

Criminal conviction data	As defined at Article 10 means personal data relating to criminal convictions and offences.
Other sensitive personal information	Personal data which could cause distress if disclosed without the data subject's permission (for example, financial information, information relating to an individual's family situation [but which does not constitute sensitive personal data]. This categorisation is likely to be subjective and, where a member of staff is unsure, they should be more cautious in the way they handle the information.
Pseudonymisation	As defined at Article 4(5) of the GDPR: "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"

6 Roles and Responsibilities

6.1 The COODOI is accountable to the Ombudsman for overall information governance. The CLADoI is the organisation's SIRO with responsibility for monitoring information risk management within the organisation.

6.2 Responsibility for managing and implementing the policy and related procedures rests with the ITM and IGM who are accountable to the CLADoI and COODOI.

6.3 Any breaches of the policy need to be communicated to the ITM or IGM as soon as possible after the breach is known.

6.4 The ITM and IGM are responsible for ensuring that all persons who have authorised access to PSOW IT systems are aware of:

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

6.5 All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity.

6.6 The Information Security Policy shall be maintained, reviewed and updated by the ITM and IGM.

6.7 Each member of staff shall be individually responsible for the security of their physical environments where information is processed or stored.

6.8 Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

6.9 Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

7 Legislation

7.1 The Ombudsman is obliged to abide by all relevant UK and European Union legislation. The Ombudsman shall comply with the following legislation and other legislation as appropriate:

- Public Services Ombudsman (Wales) act 2005
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)

- Human Rights Act (1998)
- Freedom of Information Act (2000)
- Equality Act 2010
- General Data Protection Regulation
- Data Protection Act 2018

8 Management of information, awareness and access

8.1 Categories of information held by PSOW

All information held by the PSOW falls into one of the following categories:

- Investigation casework information
- Information request casework information
- Complaints About Us (CAU) casework information
- Management team information
- Advisory Panel information
- Audit & Risk Assurance Committee (ARAC) information
- HR information
- Payroll information
- Financial and accounting information
- Supplier, building and facilities information

8.2 Management of information security

The ITM and IGM shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

8.3 Information security awareness training

- Information security awareness training shall be included in the staff induction process. This training shall include understanding of this policy in full and how it relates to the day to day activities of the member of staff.

- An annual information governance (IG) training strategy sets out the staff IG training and development requirements, including mandatory components. The strategy also includes a communications plan identifying key messages for the forthcoming year. Mandatory refresher training is identified each year and included within the organisational annual training plan.

8.4 **Contracts of employment**

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause, restricting the disclosure of confidential information gained during their employment with the Ombudsman.

8.5 **Access controls**

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data. All doors to protected areas are secured by physical lock or by the ID card entry system managed by Corporate Services.

- Reception: This is open to the public only during office hours and contains a sole PC protected by username and password.
- General Office: Authorisation for access to the PSOW open plan office may be given by any member of staff during office hours, but the visitor must be accompanied to the relevant member of staff they are visiting. The default access is for PSOW staff only plus the relevant office cleaner.
- IT Comms room: Authorisation for this access is managed by IT team. The default access is 'no access' apart from PSOW IT staff.
- Archive room: Authorisation for this access is managed by Corporate Services. The default access is 'no access' apart from Corporate Service/Casework Support and CAT Casework Officers.

8.6 **User access controls**

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information. Physical access rights are managed by Corporate Services. IT access rights are managed by the PSOW IT team.

9 Risks and Business Continuity

9.1 **Risk identification and treatment**

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence for each category of information.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the PSOW risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed by management team and reported to Audit & Risk Assurance Committee (ARAC) at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the Ombudsman's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

All teams should have 'risk identification' as a standing item on their team meeting agendas.

9.2 **Information security events and weaknesses**

All information security events, and suspected weaknesses are to be reported to the ITM or IGM. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events. The process is set out in the Information Security Incident Management Policy and Procedure.

9.3 **Business continuity and Disaster Recovery plans**

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

To assist in data recovery in the event of loss of services, the following business as usual actions must be followed:

- Soft backups (i.e. server stored) should be made by the relevant support member of staff following any session of data entry/data amendment on any locally installed business critical system e.g. accounting and payroll systems (Sage accounts and Sage Payroll)

- The PSOW IT suppliers are responsible for ensuring sufficient server mirroring, to enable short term data recovery in the event of a server/application failure.

- Backups are to be administered by IT Team in liaison with the PSOW IT service providers.

- Onsite Daily and Weekly backups: Full backups of the servers are to be made daily and weekly to the backup server (located separate to the main ground floor server room).

- Offsite backups: A copy of the most recent weekly back up is to be taken offsite by PSOW. There are three portable backups which are rotated weekly to ensure one back up is always offsite at any one time, in case of catastrophic system loss such as fire/flood (this is due to be replaced by a cloud backup solution).

- Further information can be found within the organisation's Business Continuity Plan.

10 Clear desk policy

10.1 Desk space and desk partitions

- No personal information (other than staff own personal information) or case file information is to be left out on desks unattended outside of office hours. This includes information contained within ring binders, in/out trays, 'Red' shredding trays and information pinned to desk partitions.

- For the purposes of this policy, office hours are defined as Monday to Friday 9am to 5pm (excluding bank holidays).

- Disposal of all hard copy documents that contain casework information or any other personal information must be destroyed via the use of the 'Red tray', which must be emptied daily into the large confidential waste bins.

- All 'red shredding trays' within each team are to be emptied daily before the last member of staff in that team leaves for that day. Line Managers are responsible for ensuring this process is followed.

- Individual staff's own personal information (e.g. photos, own personal contact details etc) are excluded from the above as it is the choice of the individual as to the visibility of their own personal data.

10.2 Side filers and pedestals

Desk pedestals and side filers must be locked (and keys removed and kept secure) outside of office hours if they contain case file/personal/ or sensitive information.

10.3 Security of access

Items which enable access to secure information (such as keys to live filing/side filers/passwords etc) must not be left in easily identifiable areas (e.g. on desk partitions, left in unlocked pedestals etc) outside of office hours.

10.4 **'Archive' filing and 'live' filing security**

The Archive filing will be kept in the 'Filing' room, which is always to be kept secured. Corporate Services will control access levels to Archive filing via the security ID card system. Each member of staff accessing Archive Filing or Live filing is responsible for ensuring the area is left secure after its use.

10.5 **All other filing cabinets/areas**

Any room/cabinet/drawer etc which contains sensitive/personal or case work information, or contains assets deemed valuable must kept secured outside of office hours

All original medical records must be stored securely in the fire-proof safe outside of normal office hours. Staff who are in possession of such documents must ensure they discuss secure storage requirements with Casework Support or Corporate Services before 4pm.

11 IT access rights and control

11.1 **PC use**

- Access to any PC must be password protected, this must not be shared. The system must be set up so that it will reject passwords that do not meet the required complexity standard (must include upper and lowercase characters, a number, plus also a control character e.g. $, and must be 9 characters or more in length).

- Computer screens (or mobile device equivalent) must be 'locked' when a member of staff leaves their desk and moves out of visible range of the screen. This is to protect not only personal information which may be on view, but also as protection against unauthorised access to the IT system.

- Computer screens (or mobile device equivalent) must not be left on view so members of the general public or staff who do not a justified need to view the information can see personal data.

- PCs or laptops not in use should be switched off logged off or have a secure screen saver device in use.

11.2 **Computer access control**

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities. Only users authorised by the ITM (or delegated member of the IT team) may be added to PSOW IT systems.

11.3 **Application access control**

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

11.4 **Protection from malicious software**

The organisation shall liaise with the PSOW IT suppliers for advice and recommendations with regard to adequate software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users are by default not able to install software on the organisation's property without permission from the ITM.

11.5 **USB memory stick or similar user media**

Non PSOW issued portable memory devices such as USB memory sticks or similar, require the approval of IT before they may be used on the Ombudsman's systems. Such media must also be fully virus checked before being used on the organisation's equipment. Whilst this does not apply to CD/DVDs sent from Relevant Bodies due to the lower risk of malicious content, it is still important that CD/DVDs sent in from members of the public are referred to IT to ensure there is no executable files contained within them.

11.6 **Mobile devices (e.g. laptops/tablets/smart phones)**

For business continuity and PSOW meeting purposes, the Ombudsman may issue authorised staff with PSOW owned smart phone and/or tablet PCs.

Standard PSOW policy for PC use applies to the use of these devices regarding use as stated in this policy and any other relevant PSOW policy e.g. Staff standards of conduct policy.

Staff who have authorised use of Ombudsman's mobile devices should ensure adequate security arrangements are in place for the physical security of the mobile device against theft and/or unauthorised access of any data contained within the mobile device.

- Don't use your mobile device in public where work related information can be seen 'over your shoulder'.
- Always use screensaver and password security for mobile device access, and do not divulge this password.
- Always keep your mobile device in secure locations, and never unattended where it can be seen (even if secure, e.g. in back seat of your car).
- Unless it is the most secure option available, do not leave your mobile device in the car boot while the car is unattended for extended periods especially overnight.
- Never let anyone import documents into your mobile device using unauthorised media devices. Only use known and PSOW authorised portable media devices to transfer documents.

Further details of measures to be taken can be found under the section on 'Working away from the office'.

11.7 **Monitoring system access and use**

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis by the ITM.

11.8 **Accreditation of information systems**

The organisation shall ensure that all new information systems, applications and networks are prior to installation and commencement, risk assessed for security purposes

11.9 **System change control**

Changes to information systems, applications or networks shall be reviewed and approved by the ITM.

11.10 **Intellectual property rights**

The organisation shall ensure that all information products are properly licensed and approved by the ITM. Users shall not install software on the organisation's property without permission from the ITM.

11.11 **Security control of assets**

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset when taken outside of the Ombudsman's premises.

11.12 **Computer and network procedures**

Management of computers and networks shall be controlled through standard documented IT team procedures that have been authorised by the ITM.

11.13 **Equipment security**

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards and subject to security marking. All PCs when located in the open office environment (i.e. not stored in a restricted access secure storage room) are to be secured using lock and security cable.

11.14 **Disposal of IT equipment**

An inventory of all PSOW IT equipment that is marked for disposal that has stored personal information contained within it must be maintained by PSOW IT Team, detailing the disposal company used. A written agreement is required to be in place with PSOW and the disposal company detailing the requirements for the disposal which must include mention of the disposal company as the 'data processor' under the control of PSOW as the 'data controller'. A requirement for the disposal company to destroy personal information in a secure manner and provide PSOW with a destruction certificate must also be included in the agreement.

11.15 **Emails**

Staff can use the 'autocomplete' function on Outlook, whereby Outlook suggests recipients based on previous letters selected. However, staff are responsible for ensuring that the list of recipients are reviewed regularly, with old addresses removed. Instructions are set out below:

Removing an address from the list

(i). Open a new message and begin typing the address.

(ii). Use the up and down arrow keys to select the address to be removed from the addresses suggested. When the address to be removed is highlighted, press the **Delete** key.

Switching off 'auto-complete'

(i). Select 'Tools', then 'Options';

(ii). Select 'Preferences' tab, then 'Email Options';

(iii). Select 'Advanced Email Options', then clear the check box for 'Suggest names while completing To, Cc, and Bcc fields'

12 Working away from the office (including working at home): Security of information and IT equipment

- All information and equipment must be kept secure at all times. Staff must be satisfied that adequate precautions are in place to maintain confidentiality of material in accordance with the Data Protection Act and Ombudsman's guidelines, policies and procedures.

- Where an employee takes material (for example, a hard copy case file) off premises, that employee is responsible for the material for the full period of time that it is off premises.

- Where the employee takes a hard copy case file off premises, they are responsible for updating the WorkPro record to confirm the new file location – for example, 'Homeworking – Case Owner'. The WorkPro record should be updated before the file is taken off premises.

- The 'Office Caseload' report will provide the location of all live hard copy files. The 'Closed cases file location' report (stored in the Admin folder) will provide the location of all closed hard copy files.

- The employee is responsible for ensuring that hard copy case files, and any IT equipment (including tablets or telephones) are secure at all times, including whilst in transit.

- When travelling, the employee should not leave any material or IT equipment unattended.

- Where it is necessary to leave material or IT equipment unattended, this should be stored securely and out of sight. Files should not, for example, be left on the back seat of a vehicle when unattended and should be moved into the secure boot area and locked away.

- Employees must keep all information confidential and secure. The Information Security Incident Management Policy Procedures should be followed in the event of any losses or potential risks to information.

For example, a break in or attempted break in. Incidents or risks should be reported to the ITM or IGM. Employees must not show (or allow to be shown) any data to any members of their family or visitors to the household.

- When viewing confidential or sensitive information in transit (e.g. on public transport) staff should ensure that they cannot be overlooked by other passengers.

- The Ombudsman is not responsible for any costs associated with the user's own IT equipment i.e. purchase, installation, maintenance, internet/telephone fees.

- The Ombudsman is not responsible for any costs associated with repair in the event of loss or damage to any personal equipment that the employee uses.

- IT assistance will only be available from the IT Team during normal "core" office hours and will relate solely to configuration settings connecting to the Ombudsman server.

- Any IT issues which do not relate directly to configuration settings connecting to the Ombudsman server are the user's responsibility to resolve. For example, inability to connect to internet via the user's internet provider is not the Ombudsman's responsibility. Staff should work via the secure remote access portal and WorkPro for any casework related documents. If it is considered necessary to work temporarily outside of the WorkPro portal, users must ensure any documents saved on their own personal PC/laptop etc are uploaded to WorkPro and fully deleted from their own device at the end of the session.

- All material taken off premises should be returned immediately following the completion of the agreed period of time working at home. Where an employee works at home for an extended period of time, they should return any files not in ongoing use as soon as possible.

- The employee should not destroy or dispose of any material through domestic household waste. All material should be returned to the office and destroyed using PSOW confidential waste bins.

13 Secure handling of correspondence

Correspondence: Outgoing postal/courier/email

- This section details how to transmit information once the information has been assessed as being authorised to transmit in accordance with relevant legislation e.g. Data Protection Act, PSOW Act etc. Please refer to ITM if you are in doubt.

- This section of the policy refers to the following members of PSOW staff;
  - the REQUESTER: This is the member of staff who is requesting information to be sent.
  - the SENDER: This is the member of staff who actions the request from the REQUESTER. This person may be the same individual as the requestor.

- The requestor must follow the guidelines set out in Appendix A of this policy and instruct the sender accordingly.

- All information contained within outgoing correspondence whether sent via normal post, courier or e-mail must be checked thoroughly by the requestor for the following:

  - correct recipient details.

  - correct content (including all attached documents).

  - In the case of emails that any historic thread and its full contents are appropriate to be communicated to the intended recipients (including CC and BCC recipients).

IMPORTANT NOTE: It is PSOW policy that the requestor removes all internal email exchanges contained within the historic email thread before sending any email outside of PSOW. This applies to all PSOW staff and all PSOW emails and not just emails concerning investigation cases.

- Does any of the content contain any sensitive personal information?

- When a case is new to a caseworker, and the caseworker is sending an email or letter to a person involved in a complaint for the first time, that member of staff must check that the email or letter is correctly addressed against an original source which has been provided by the complainant or the appropriate person. For example:

  - a complainant's postal/email address must be cross-checked against the original complaint form or letter;

  - an accused member's postal/email address must be cross-checked against information received from the relevant council or clerk;

  - a witness' postal/email address must be cross-checked against information received from either the witness themselves or the person who has provided their contact details.

- The sender is responsible for ensuring that:

  - the caseworker is given the final letter (which will list all enclosures at the end of the letter after the signature) together with all of the documents enclosed so that the caseworker can cross check these documents when signing the letter.

  - no additional documents/information is sent in addition to that which has been requested.

- the recipient is as requested, the address matches that as per the WorkPro case record for the intended recipient (on the basis that the caseworker will have already checked that the postal or email address against an original source provided by the complainant or the appropriate person).

- If there is any concern about the content and how it has been requested to be sent that it is referred back to the requestor e.g. the sender identifies that the requestor has requested that a document is sent in a manner which is contrary to Appendix A guidelines.

- Staff should use Egress secure email for sending confidential or sensitive personal information securely. Please refer to the Egress process for more information.

- Staff can send pseudonymised data without the need for encryption.

- Staff should use Egress for all correspondence with Independent Professional Advisers. Please refer to the IPA process for more information.

Correspondence: Incoming via post/courier

- Security of opening mail – all staff that are responsible for opening mail should be aware of and follow the suspicious package procedure.

- Staff should be aware that all written correspondence (except those noted in section 13.16 to 13.20) that is received at the Ombudsman's premises could be opened, irrespective of the markings on the envelope. Correspondence addressed to a named individual in their capacity as a member of the PSOW, belongs to the Ombudsman who has delegated responsibility for processing it to departmental management.

- If a member of staff requires personal correspondence to be sent somewhere other than their home address, they should make appropriate arrangements with the Post Office in the first instance.

In exceptional circumstances staff may arrange or allow personal correspondence or parcels to be sent to the Ombudsman's offices, however staff must be aware that it may be opened and that the Ombudsman will not accept any liability for any damage or loss of any contents at any stage.

- There will be occasions when it is necessary for personal correspondence to be sent within the organisation and it would not be appropriate for anyone, other than the addressee, to open that correspondence. This may include information on pay, pensions, complaints, grievances and a range of Human Resources issues. Internal correspondence that is of a personal nature sent between individuals within the office should be marked 'Restricted – Addressee Only' on the envelope.

- All members of staff that open correspondence have a responsibility to maintain confidentiality.

- Article 8 of the Human Rights Act 1998 – Right to respect for private and family life – gives everyone the right to respect for their private and family life, home and correspondence. This is not, however, an absolute right and the Ombudsman has to balance any interference with the right against the legitimate aims that are being pursued. If correspondence is not opened this could have serious implications for the services that the Ombudsman provides

Correspondence that should not be opened by any person other than the named recipient

- Internal correspondence that is marked ''Restricted – Addressee Only''.

- Correspondence that is marked 'private' and/or 'confidential' and is addressed by name to the Ombudsman e.g. 'Private & Confidential, Nick Bennett' (i.e. not "the Ombudsman").

- All correspondence that is addressed to ‘Corporate Services’ should be forwarded on unopened to Corporate Services as this may contain personal HR information about PSOW staff.

- All correspondence that is marked ‘for union official only’ should only be opened by the relevant union representative.

- Any other correspondence where it is obvious that it is not work related (e.g. correspondence from staff associations/unions, correspondence from pension providers marked “personal”). In these instances, the correspondence should be forwarded directly to the addressee (or Ombudsman PA for second point above).

Correspondence that may be opened

- All other correspondence may be opened, including correspondence marked ‘private and confidential’ and addressed to an investigator/case officer as most complainants would address such correspondence to case officers as private as a matter of course.

- Where mail that is opened is subsequently found to be of a personal nature, it should be signed and endorsed with the reason for it being opened and forwarded to the addressee, stating ‘Restricted – Addressee Only’ on the envelope and in a new sealed envelope where appropriate.

- Incoming medical records need to be opened carefully without damaging the original envelope as this may be needed to be retained (e.g. X-Ray folders) for when sending on/returning the documents.

- All mail (except X-Ray envelopes which must be retained for returning the X-Rays) should be opened by fully ‘splaying’ the incoming envelope to ensure no contents are missed or left within the envelope. This includes ‘Jiffy bag’ envelopes. All opened envelopes are to be placed in confidential waste after a second check to ensure all the envelope contents are removed. Under no circumstances are envelopes or ‘jiffy bags’ to be re-used.

- Corporate Services and Casework Support are responsible for maintaining the internal process for handling incoming post, which should also cover incoming portable media.

Incoming caller verification

- Staff should verify the identity of callers wishing to obtain passwords. Staff should request two items of information that the complainant (or representative) is likely to know – for example, name, address, postcode, body complained about, or any other item of information which the staff considers the complainant (or representative) is likely to know. Staff should not disclose passwords unless they are satisfied that a verification test has been passed.

Facsimile transmissions and 'Safe Haven'

- PSOW now operates an electronic facsimile system that is classified as a 'Safe Haven' service for incoming documents as it is accessible via a secure password protection method.

- Outgoing documents that contain personal information must only be sent via this system following the express consent of the recipient on the condition that the personal information solely relates to them and not a third party. The sender must contact the intended recipient before sending, to ensure that the recipient is able to take immediate receipt. The sender should also contact the recipient after sending to confirm safe receipt. The Corporate Service Manager or IT Team must be informed of any instances where there is doubt the transmission has been successful to enable an IT audit check of where the document was transmitted to.

14 Reporting & Audit

- **Assurance**

  Whilst information security is a daily consideration of the ITM and IGM and that the ITM or IGM shall keep the Management Team informed of any issues that seriously affect the information security status of the organisation, there will also be an annual report to management team and subsequently to the Audit & Risk Assurance Committee which will contain the following:

  - IT access: external penetration tests
  - IT access: internal compliance with this policy
  - Monitoring of visitors
  - Compliance testing on transfer of information
  - Any data loss incidents and subsequent actions since the last report

- **Information Security Incident Management**

  In the event of a reported or known incident involving the loss of, or revealing in error confidential data (whether in electronic or physical files) held by the PSOW the following procedure is to be followed:

  - As set out in the Information Security Incident Management Procedure, the incident must be reported to the IGM or ITM as soon as it comes to light. [ISIM Procedures currently being revised]. The incident form should be completed.

  - The IGM or ITM should review the completed form. The incident should then be referred to the COODOI and SIRO.

  The IGM (or the ITM if the incident relates to IT security) is to report the incident and subsequent actions to the Management Team as part of the monthly report. Where appropriate, the incident should also be reported to the Audit and Risk Assurance Committee.

The line manager must be notified of the incident to consider any necessary steps (informal or formal), taking into consideration (where necessary) any appropriate policies, including the Performance Management Policy and the Disciplinary Policy. However, any necessary actions should not be listed on the form, which may be disclosed to the Information Commissioner's Office in the event of notification of the breach.

15 Appendix A: Correspondence via email and post

<table>
<tr><td>Start</td><td colspan="6"></td></tr>
<tr><td rowspan="2">Is it an original record or original certificate</td><td rowspan="2">Yes</td><td rowspan="2">X-rays?</td><td>Yes</td><td colspan="3">A</td></tr>
<tr><td>No</td><td colspan="3">B</td></tr>
<tr><td>No</td><td colspan="6"></td></tr>
<tr><td rowspan="2">Does the content contain special category data, criminal conviction data or other sensitive information (e.g. financial) likely to cause damage or distress if disclosed inadvertently?</td><td rowspan="2">Yes</td><td rowspan="2">Hard copy or email?</td><td rowspan="2">Hard copy</td><td rowspan="2">Can it fit into an A4 envelope?</td><td>Yes</td><td>C</td></tr>
<tr><td>No</td><td>D</td></tr>
<tr><td>No</td><td>↑</td><td colspan="5">Email</td><td>E</td></tr>
<tr><td>Multiple items of personal data (e.g. names, addresses, etc)?</td><td>Yes</td><td colspan="5"></td></tr>
<tr><td>No</td><td colspan="6"></td></tr>
<tr><td rowspan="2">Hard copy or email?</td><td rowspan="2">Hard copy</td><td rowspan="2">Can it fit into an A4 envelope?</td><td>Yes</td><td colspan="2">F</td></tr>
<tr><td>No</td><td colspan="2">D</td></tr>
<tr><td></td><td>Email</td><td>G</td><td colspan="3"></td></tr>
</table>

A	Tracked courier. If possible, X-rays should be sent in the original packaging in which they were received and put inside a further envelope or box marked 'Private and Confidential'
B	Tracked courier
C	Normal post but marked as 'Private and Confidential'
D	Tracked courier
E	Egress (in exceptional cases, the document can be password-protected using pdf software instead)
F	Normal post
G	Normal email

The above are minimum requirements. Staff can at any time elect to send the information using a higher level of security.

For C & F: Staff may request recorded royal mail delivery if proof of delivery is required e.g. upcoming deadlines

For E: If in doubt, staff should use courier or encrypt.

16 Appendix B: Email good practice

1. **Subject header**
   The subject header should always contain the reference number but no personal information. Examples of the PSOW standard subject headers for emails is shown below:

   - Case ID - 201999999 - Acknowledgement
   - Case ID - 201999999 - Response to your query
   - Case ID - 201999999 - Draft decision
   - Case ID - 201999999 - Response to draft decision comments
   - Case ID - 201999999 - Review response

2. **Sending via Egress or Outlook**
   This depends on whether the information within the email contains personal information (not including the name of the recipient and their email address). The table at the start of Appendix A should help you decide whether to use Egress or Outlook to send your message.

   You can send emails from within WorkPro. Doing so has the advantage of:

   - The email subject title will already have the 'Case ID - 201499999' populated
   - There is no need to consider email threads
   - There is no need to manually manage emails within your Inbox

3. **Email chains**
   Unless it is considered essential for the recipient it is best to avoid long email chains. You can start a fresh email but reference the correspondence that you are replying to e.g. “Thank you for your email of XXXX…”

4. **Managing emails**
   Emails need to be saved to the relevant record wherever possible. This ensures that those records are accurate and kept up to date with the latest correspondence. Emails that are kept in an individual or team Inbox are not accessible to others in PSOW who have a legitimate reason to access the record.

   All case related emails must be uploaded to WorkPro. The email may then be deleted from the user’s Inbox.

   Refer to the Records Management Policy and accompanying record retention schedules for the relevant retention period for the different types of records [currently under review].

5. Email signatures

All staff should use the standard PSOW signature for emails to external recipients:

Staff Name
Job title in English / Job title in Welsh
Tel / Ffôn: 01656 64XXXX

All outgoing emails automatically include the following statement:

--
Public Services Ombudsman for Wales/Ombwdsmon Gwasanaethau Cyhoeddus Cymru
1 Ffordd yr Hen Gae
Pencoed
Bridgend/Pen-y-Bont ar Ogwr
CF35 5LJ

www.ombudsman-wales.org.uk

This email is subject to the conditions on Confidentiality, Content and Viruses set out on the Ombudsman's website.
Mae'r e-bost hwn yn rhwym wrth yr amodau Cyfrinachedd, Cynnwys a Firysau a nodir ar wefan yr Ombwdsmon.

All calls are recorded for training and reference purposes / Bydd pob galwad yn cael ei recordio ar gyfer dibenion hyfforddi a chyfeirio

Please consider the environment - do you really need to print this email?
Ystyriwch yr amgylchedd - a oes wir angen i chi argraffu'r neges e-bost hon?