

WELSH GOVERNMENT SECURITY POLICY



Owner:	Kath Jenkins
Issue Number:	6.0
Date:	11 November 2025
Next Review Date:	11 November 2026

Contacts:	Kath Jenkins via securitypolicy@gov.wales
Policy Owner:	Kath Jenkins, Chief Security Officer
Publication:	This policy is located on the Welsh Government Intranet at: https://wales365uk.sharepoint.com/sites/Intranet-Security-Managing-Information/SitePages/Security-Policy-and-Departmental-Security-Unit.aspx
Supporting Information:	Release Notes

Who is this policy for?

Everyone who has access to buildings, assets, information and IT systems/equipment (including telephones and removable media) within the Welsh Government including Welsh Revenue Authority (WRA).

What is this policy about?

This policy sets out the appropriate standards of behaviour expected by everyone who has access to buildings, assets, information and IT systems (including telephones and removable media) within the Welsh Government. Failure to meet these standards may lead to disciplinary action.

Table of Contents

1. Introduction.....	4
2. Breaches of the Security Policy	4
3. Monitoring.....	5
4. Protecting and Sharing Information	6
You must:	6
4.1 Records Management / iShare	6
5. Protecting our IT	7
5.1 IT Equipment	7
5.2 Email.....	8
5.3 The Internet / Social Media / AI Tools.....	9
5.4 Telephones (including smartphones, tablets and other mobile devices).....	9
5.5 Collaboration Tools.....	10
6. Personal Use of IT Equipment – laptops, email, smartphones, phones, printers etc.	11
6.1 Copyright Law.....	11
6.2 Examples of appropriate and inappropriate personal use	12
7. Working Securely	13
7.1 Securely Store Paperwork and IT Equipment.....	13
7.2 Working / Travelling Overseas.....	15
8. Maintaining Physical Security	15
8.1 Reporting Security Incidents and Emergencies	15
8.2 Security Passes	15
8.3 Visitors.....	16
8.4 Postal Mail	17
8.5 Opening of Personal Lockers	17
8.6 Photography / Video	17
8.7 Vehicle Passes, Bicycles and Car Parks	19
9.1 Security Clearance (Vetting).....	19
10 WRA Section	20
Annex A – Examples of Misconduct and Gross Misconduct	22
Annex B – Inspectors.....	27
Annex C – What personal devices can I connect to my laptop?	28
Annex D – Authorised Lanyards	30

1. Introduction

This policy sets out the appropriate standards of behaviour expected by everyone who has access to Welsh Government buildings, assets, information and IT equipment¹.

The Welsh Government Security Policy applies to all staff, including secondees, staff on placement, contractors and consultants. The Security Policy forms part of your terms and conditions of service. The requirement to comply with the policy is included in employment contracts and agreements.

It is your responsibility to ensure you comply with the Security Policy and any other policies which apply to your work. You are also responsible for ensuring that you undertake any mandatory training.

In this document, a reference to the Welsh Government also means a reference to the Welsh Revenue Authority (WRA) when applying this policy. Some parts of this policy will only be applicable to WRA activities and these are set out in Section 10.

As risks change, new security issues will inevitably arise and you must follow the principles and spirit of this policy to decide what is appropriate and acceptable behaviour.

2. Breaches of the Security Policy

Failure to comply with this policy may result in disciplinary action. Any suspected cases of misconduct will be investigated by Welsh Government.

You must report all known or suspected breaches of this policy without delay, following the procedures in the [Reporting Security Incidents and Emergencies](#) guide.

On no account must you attempt to cover up a security incident or attempt to limit any damage or embarrassment caused to you or to others before reporting it.

Any allegation of a breach to the Security Policy will be investigated by the Departmental Security Unit on the instruction of Human Resources.

¹ The term 'IT equipment' applies to any Welsh Government owned IT device (whether fixed, mobile, telephony, physical or virtual) or network.

Breaches of the Security Policy are regarded as serious and may result in disciplinary action, including possible charges of misconduct or gross misconduct.

You must co-operate fully and truthfully in any security investigation irrespective of your status in the investigation e.g. the subject of the investigation or a witness.

We will co-operate fully with the police or government officials of an appropriate level in any investigation relating to unlawful activities conducted using Welsh Government IT equipment or systems.

We will notify the police as appropriate of acts we believe to be illegal and will disclose evidence to them where there is reasonable suspicion of criminal activity.

If an investigation proves that you have accessed material that is pornographic, advocates illegal acts, violence or discrimination towards other people, this could be considered gross misconduct. Disciplinary procedures will be initiated which may lead to sanctions up to and including summary dismissal.

Examples of behaviours that are considered to constitute misconduct or gross misconduct are outlined at Annex A.

3. Monitoring

Any information you create or communicate using Welsh Government IT equipment is not private and may be read, listened to or copied by the Welsh Government without notice.

Monitoring is undertaken for the following reasons:

- i. To help maintain compliance with practices or procedures set out in law;
- ii. To establish facts and protect the interests of the Welsh Government;
- iii. To prevent unauthorised use of IT systems;
- iv. To prevent inappropriate/offensive media being stored on, or communicated using the IT systems;
- v. To assist with any investigation or action proposed by lawfully authorised investigating or regulatory bodies (e.g. police);
- vi. To comply with access to information obligations under, e.g. UK GDPR and the Freedom of Information Act 2000;
- vii. For quality control and staff training purposes.

Welsh Government also reserves the right to make and keep copies of all information, (including, but not limited to, system usage such as logon/off times, location information, telephone calls, Teams and other electronic

content, email and data documenting use of the telephone, email, internet systems, applications or removable media) for the purposes set out above, and if it sees fit, to use the information in disciplinary proceedings.

The Departmental Security Unit will make periodic spot checks to ensure that the policy is being followed and interpreted correctly. Any breaches discovered will be recorded and reported to Human Resources.

4. Protecting and Sharing Information

You are responsible for protecting the information that you handle and sharing it in a secure manner.

You must:

- i. Complete the Civil Service Learning Course: Security and Data Protection Fundamentals (available from the Learning Lab) at the start of your employment and the Refresher course at regular intervals as directed via corporate communications or your business area. The interval is usually every 2 years, although some areas of Welsh Government require its completion every 12 months.
- ii. If you are taking OFFICIAL-SENSITIVE hard copy information out of the office, then you must always have your Information Asset Owner's (IAO) approval or Line Manager approval if your IAO is not contactable.
- iii. If you are handling SECRET information or dealing with information relating to COBR meetings, you must adhere to the [Handling SECRET information Policy](#).
- iv. Follow the correct procedures for handling, sending and disposing of information:
[How do I ...Handle and Dispose of Information](#)
[How do I ...Send Electronic Information Securely](#)
[How do I ...Send Hard Copy Information Securely](#)
[How do I ...Use Government Security Classifications](#)
- v. Report any data breaches as soon as you become aware of the breach following the procedures in the [How do I ...Report and Manage Data Breaches and Near Misses](#) guide.

4.1 Records Management / iShare

You must:

- i. Save all information in iShare or other approved document management system e.g. customer relationship management (CRM) systems. This will

- ensure that information is available even when you are not. Remember that OneDrive is temporary storage only and not an alternative to iShare;
- ii. Only use your iShare 'My Home' folder to store personal information related to your work, your role or personal development e.g. details of leave, flexi time or documents related to work-sponsored courses;
 - iii. Make sure hardcopy sensitive information and portable IT equipment is stored securely when not in use. See Section 7 for how to store paperwork and IT equipment;
 - iv. Immediately tell your Line Manager if you come across sensitive documents (e.g. during an iShare search or left at a Business Point) which you would not expect to see as part of your role;
 - v. Do not destroy registered files. This may only be carried out by the Information and Records Management team.

5. Protecting our IT

You are responsible for taking care of the IT equipment that you use and for safeguarding any login credentials, passwords or PINs that have been allocated to you.

5.1 IT Equipment

You are personally responsible for any IT equipment allocated to you. Welsh Government maintains an audit trail of activity conducted on its network.

Section 6 provides examples of appropriate and inappropriate personal use of IT equipment (including email, internet, social media, telephones and collaboration tools).

Welsh Government retains full remote access rights to all the devices where its information is stored to maintain the security of those devices.

Laptops, smartphones and mobile devices should be switched on to receive automatic updates at least once every two weeks. Should you choose to retain your device whilst away for any long-term reason (e.g. whilst on parental leave) then your device may require a long restart period or to be returned to IT Services for manual updates to be applied.

You must:

- i. Never use a personal IT device for sharing or processing official business, joining business meetings or attempting to connect to corporate systems;
- ii. Immediately report any misplaced, lost, stolen or damaged equipment to the IT Service Desk;
- iii. Always store IT equipment e.g. laptops, iPads, cameras, mobiles and removable media in a secure location. See Section 7 for how to store paperwork and IT equipment;

- iv. Only attach devices to the corporate network or IT equipment that have been approved through the IT Service Desk or those listed in Annex C;
- v. Store passwords and PINs separately from IT equipment (including shared equipment);
- vi. Lock your computer screen whenever you leave your desk and also power down your laptop at the end of the day;
- vii. Not allow anyone else (e.g. a colleague) to use your IT equipment (laptop, smartphone, mobile phone etc) when you are not present;
- viii. Not allow anyone else, e.g. a visitor, colleague, friend or family member to use your username/password/PIN;
- ix. Not allow anyone without allocated Welsh Government equipment of their own e.g. contractor, friend, family member to use your IT equipment (laptop, smartphone, mobile phone etc) even if you are present;
- x. Change your password or PIN immediately if you suspect that it has become known to anyone else;
- xi. Return corporately owned IT equipment (raise a request on MyIT) when you no longer require them;
- xii. Raise a MyIT request if any fault develops on Welsh Government IT equipment or if fixed assets e.g. printers, docking station, monitors need to be moved;
- xiii. Ensure that you do not connect personal IT devices that process data (e.g. phones, tablets, memory sticks) to Welsh Government equipment. This includes:
 - charging your mobile phone via your laptop's USB port;
 - charging your mobile via a personally owned dock/USB port extender whilst your work laptop is connected to the dock/USB port extender;
 - connecting a personally owned device to a Welsh Government docking station;
- xiv. Charge Welsh Government mobile devices via a 3 pin plug. Note: you may charge personally owned electronic mobile devices e.g. phones in the office via a 3 pin plug.

5.2 Email

You must:

- i. Only use Welsh Government email for official business, except in the case of an emergency;
- ii. Only use Welsh Government IT equipment and your Welsh Government email address to conduct official business. You must not use any other address for official business e.g. gmail;
- iii. Delete any non-work related images that you may receive via email without forwarding them (even unopened) to any other email address;
- iv. Use the standard out-of-office message to provide alternative Welsh Government business contact details for work related purposes if you are away from work;
- v. Use the standard out-of-office reply feature and do not create any other auto-forward or reply rules.

- vi. Bcc email addresses when sending information or meeting invitations to a group which includes external people so that personal email addresses are not shared (unless all recipients have agreed to share their contact details with each other).

5.3 The Internet / Social Media / AI Tools

Welsh Government may access publicly available information on social media sites during investigations.

You must:

- i. Comply with the procedures set out on the social media intranet pages if you use social media in an official capacity. In particular:
 - only use a Welsh Government social media account from Welsh Government IT equipment;
 - do not change the registered email address associated with the social media account to a personal email address;
 - do not share any passwords with a third party;
 - use two factor authentication where it is available.
- ii. Leave the website immediately and notify your Line Manager if you accidentally access an offensive website which could bring Welsh Government into disrepute while using Welsh Government IT equipment;
- iii. Only download software from the Company Portal.
- iv. Not use personal social media accounts to promote your Welsh Government role. It is strongly recommended that you remove Welsh Government as your employer from all personal social media profiles (with the exception of work-related social media e.g. LinkedIn).
- v. Not conduct official business on Non-Corporate Communication Channels (NCCC) e.g. WhatsApp, Signal, private email, private messaging, Facebook or LinkedIn etc. If an exchange on an NCCC strays into official business:
 - it must be halted and resumed on your corporate device;
 - a copy of the conversation must be saved to iShare.
- iv. Only use approved versions of Artificial Intelligence (AI) tools when working with OFFICIAL-SENSITIVE or personal data. A list of approved tools is available on the [intranet](#). Check the list regularly as the tools do change as the technology develops. If using an AI tool that isn't on the approved list, only enter information or queries that would not cause any embarrassment to the Welsh Government if the exchanges were published in full.

5.4 Telephones (including smartphones, tablets and other mobile devices)

Like email, Welsh Government telephony (either from physical handsets or Teams voice via laptops) is provided for the purpose of undertaking official business but may be used in an emergency. They are not a substitute for a personal device. Mobile numbers cannot be transferred to an individual when they leave the Welsh Government.

You must:

- i. Use all available security devices such as keypad locking codes and PIN codes to prevent unauthorised use in the event of loss or theft;
- ii. Not loan or transfer a smartphone or mobile device that has been issued to you to anyone else e.g. work colleague, contractor, friend or family member;
- iii. Not allow anyone else e.g. a colleague to use your Welsh Government device when you are not present;
- iv. Not allow anyone without allocated Welsh Government equipment of their own (e.g. contractor, friend, family member) to use your device even if you are present;
- v. Only download Apps from the Company Portal.

5.5 Collaboration Tools

The Welsh Government has a number of approved collaborative tools such as iShare Connect (for sharing documents with third parties) or Teams (for audio video calls and chat messages).

Note that your contributions to video calls and chat/instant messages are in scope of Freedom of Information requests and Data Protection Legislation.

You must:

- i. Only **host** meetings using corporately approved tools i.e. Microsoft Teams;
- ii. Obtain approval before using any new collaborative tool. See the [Security Aspects of Using Collaborative Tools Policy](#) for further information;
- iii. Only use Zoom to **attend** a meeting hosted by a third party;
- iv. Only discuss information in the public domain (or information about to go into the public domain) if you join a Zoom meeting hosted by a third party;
- v. Save Teams chat messages that have a business value to iShare e.g. by taking a screen shot of the relevant messages;
- vi. Assume that your calls involving external participants using any collaboration tool are insecure. You have no control over how the third party may record the call or store the content of chat messages;
- vii. Never give an external participant (someone without a gov.wales account) control of your screen;
- viii. Never allow another Welsh Government staff member control of your screen unless you are present the entire time;
- ix. Only use Teams collaboration with third parties in accordance with [published procedures](#);
- x. Behave appropriately, the [Dignity at Work](#) policy applies to all communications;
- xi. Be proactive when hosting a meeting with external participants and check whether AI bots have joined, manually removing any that appear. (Look for participants with a [hexagonal avatar](#) and periodically check the meeting participant list for unusual names).
- xii. Use a profile picture which is a true likeness of yourself e.g. you must not use pictures of celebrities, cartoons or places.

6. Personal Use of IT Equipment – laptops, email, smartphones, phones, printers etc.

Welsh Government IT equipment is provided primarily for official business. They are not a substitute for a personal device.

Welsh Government IT equipment is provided primarily for official business. The two exceptions to this rule are that:

- i. IT equipment can be used for personal use in the case of an emergency e.g. to deal with caring responsibilities that arise during work time.
- ii. Limited **internet browsing** is permitted during non-working hours (e.g. lunch time and when travelling away on business).

All personal use of Welsh Government IT equipment is carried out at your own risk. Welsh Government accepts no liability for any loss or damage arising from personal use of its IT systems/equipment.

Any personal use of Welsh Government IT equipment which affects the performance of the IT systems or which breaches copyright law has the potential to bring the organisation into disrepute could result in disciplinary action.

6.1 Copyright Law

Copyright law is complex and covers screens e.g. TVs as well as other devices such as laptops, mobiles and tablets. This section of the Security Policy applies to copyright for any audiovisual resources accessed via Welsh Government devices. Other aspects of copyright law are detailed in the [Information Management and Governance Policy](#).

Welsh Government has a corporate TV licence that allows staff who are **physically located in a Welsh Government office** to watch **live** TV on any channel (including YouTube) and all BBC iPlayer content.

If you are not in a Welsh Government office but in another location e.g. your home, then you must ensure that if you are using a Welsh Government device (e.g. laptop to watch live TV or BBC iPlayer content) that the property has its own TV licence.

The corporate TV licence does not cover the **broadcasting** of channels on TVs (e.g. in reception areas, coffee bars) except for BBC News, Sky News, BBC Parliament, Senedd TV or any content owned by Welsh Government. For example, TVs in reception areas must not be used to play BBC iPlayer or YouTube content.

Other audiovisual content from online media and streaming channels e.g. YouTube may be used where the material is Crown Copyright or held under an open licence i.e. free for anyone to use. You must not assume that because a programme is available on the internet that it is not covered by copyright. It is your responsibility to check the copyright status of online media prior to its use.

Welsh Government's devices e.g. laptops, mobiles, tablets must not be used to view films, television programmes and other audiovisual content for which copyright licences are required. Copyright licences (other than the corporate TV licence) are not in place for your devices and if you view any other content (whether for work or personal use), then you risk infringing copyright and will be subject to disciplinary action.

6.2 Examples of appropriate and inappropriate personal use

The following table does not provide an exhaustive list but gives an indication of the types of behaviour considered to be appropriate/inappropriate use of Welsh Government IT equipment.

Example	Appropriate / Inappropriate Use
Emails to colleagues that include social chats e.g. to organise a catch-up or get together or to ask how they are if they have been away.	✓
Using Teams for: - catch-up conversations with colleagues or team social events; - training courses where Welsh Government has sponsored the activity.	✓
Using a Welsh Government telephone in an emergency to manage a caring responsibility or support your own wellbeing if you don't have access to your own phone, e.g. - take a call from a doctor when your personal mobile phone has a low battery charge or the phone signal is poor; - calling a breakdown or emergency service (AA, RAC etc).	✓
Using AI tools listed on the intranet for OFFICIAL-SENSITIVE or personal information. Only enter information that is already publicly available into other Generative AI tools such as ChatGPT.	✓

Using your Welsh Government email address for personal matters, e.g. - emailing friends/family, your builder, child's school, solicitor; - internet shopping, setting-up banking accounts, arranging insurance quotes.	×
Printing personal information not connected with work e.g. tickets, home and car insurance details, returns labels for online shopping.	×
Using Welsh Government IT equipment (laptop, smartphone, tablet etc) for personal video calls e.g. joining a family quiz, an online class or broadcast not sponsored by the Welsh Government.	×
Accessing internet sites that could bring the Welsh Government into disrepute e.g. drugs, dating sites, alcohol, replica firearms, lingerie.	×
Using your iShare Handy or My Home folders to keep copies of personal documents e.g. home and car insurance, internet purchase confirmations, personal legal or financial documents.	×
Connecting your personal IT devices (e.g. phones, tablets, memory sticks) to Welsh Government equipment. For example, if you need to charge your personal mobile phone when in the office then only do so via a 3 pin plug.	×

7. Working Securely

You are responsible for protecting Welsh Government information and IT equipment when working away from the office.

7.1 Securely Store Paperwork and IT Equipment

Paperwork and portable IT equipment must be stored securely when not in use.

In the office:

- i) Store paperwork/IT equipment securely e.g. in a locked desk drawer or cupboard once you have logged off for the day in order to comply with the [Clean Workspace Policy](#).
- ii) Use headphones if your conversations can be overheard by others.

In a coworking/collaboration space:

Coworking/collaboration spaces will be used by a variety of organisations so you should take the same level of care as you would if you were working from another public location e.g. café or public transport.

- iii) Be aware of your surroundings, make sure that your paperwork and screens cannot be viewed by others and avoid discussing sensitive matters by phone or video call;
- iv) Do not leave paperwork/IT equipment unattended. Take your laptop with you when you leave the desk, unless a locking mechanism is provided;
- v) Do not connect any device to the laptop other than a mouse, monitor, keyboard and headphones e.g. do not connect to a printer even over Wi-Fi;
- vi) Use headphones if your conversations can be overheard by others.

At home:

- vii) Store paperwork/IT equipment in a place where it cannot be accidentally damaged or used by another member of the household e.g. do not store the paperwork/IT equipment in your hallway or another room that visitors have access to;
- viii) Ensure that no-one else uses your IT account when you are not present by locking your computer (Ctrl-Alt-Del) if you leave it for a short period of time e.g. coffee break. Likewise, do not leave sensitive paperwork unattended even for a short period where others can access it.
- ix) If you deal with sensitive or personal information, then you should disable listening devices such as Amazon Alexa or Apple Siri. If you have internet enabled devices in the area in which you work that respond to voice commands, then you should discuss the suitability of your home working environment with your Information Asset Owner.
- x) If using a personal printer and shredder then you must comply with the [Printing Solutions](#) guidance and have your IAO's approval to print OFFICIAL-SENSITIVE documents.
- xi) Use headphones if your conversations can be overheard by others.

Travelling to and from the office or appointments:

- xii) Be aware of your surroundings by making sure your paperwork and screens cannot be viewed by others;
- xiii) Do not leave paperwork/IT equipment unattended e.g. on a train seat when you go to the buffet carriage or visible in an empty vehicle e.g. on the seat;
- xiv) If paperwork/IT equipment is left unattended in a vehicle, even for a short period of time, it must be locked out of sight e.g. the boot of a car. You must never leave paperwork/IT equipment in a vehicle overnight.
- xv) Use headphones if your conversations can be overheard by others.

Inspections:

- xvi) Annex B details the rules for Inspectors (HIW and CIW) visiting premises where secure storage for paperwork/IT equipment may not be possible.

7.2 Working / Travelling Overseas

If travelling abroad for work purposes:

You must:

- i. Follow the security procedures in the [How Do I ...guide to Working and Travelling Overseas](#);
- ii. Approval must be obtained for working overseas whether for work or personal reasons. If you are travelling overseas for personal reasons, authorisation will only be granted in exceptional circumstances.

8. Maintaining Physical Security

You are responsible for protecting any Welsh Government passes or keys that have been issued to you and for helping to maintain security at Welsh Government office locations.

8.1 Reporting Security Incidents and Emergencies

For further information please refer to the [Reporting Security Incidents & Emergencies](#) guide.

You must:

- i. Remain vigilant at all times and report all suspected or detected security incidents without delay;
- ii. Follow the instructions given by Security, your Local Facilities Team, and Fire Marshals or over the public address system in the event of a building alert.

8.2 Security Passes

A permanent building pass is issued to all staff, contractors and tenants once the security vetting appropriate to the post occupied has been carried out. Your pass is issued solely for your own use and must not be shared with anyone else.

You must:

- i. Wear your pass and authorised lanyard (Annex D) visibly at all times while on Welsh Government premises and remove it promptly when you leave the office;
- ii. Make sure your pass is not visible outside of the office, e.g. during a lunchtime walk or when returning to your car;
- iii. Only use your own pass;

- iv. Safeguard your pass at all times and immediately tell your local security office or Facilities Team if you have lost or misplaced it, so that it can be deactivated;
- v. Keep your pass separate from alarm fobs, office door keys or anything else which might reveal your place of work – do not attach your pass to anything showing your place of work;
- vi. Return your pass when no longer valid/required - e.g. if you leave Welsh Government employment or if the pass has otherwise expired.

Keys

Unauthorised persons should not be given the opportunity to handle or examine keys which will give them access to areas of the office/storage cupboards/filing cabinets, where sensitive material is stored. These keys and areas should only be accessible to authorised staff.

You must:

- i. Report the loss of keys immediately as detailed in [Reporting Security Incidents and Emergencies](#);
- ii. Lock keys that give access to secure areas/storage cupboards/filing cabinets in a combination lock cupboard, or in a secured key box. Keys that give access to personal storage e.g. cupboards/pedestals may be taken home with you.

8.3 Visitors

Individuals who have a legitimate business need to access Welsh Government premises may be signed in as official visitors. All visitors must have a 'lead official' who acts as a contact point and has responsibility for visitor conduct whilst they are on site. All visitors to Welsh Government will be issued with a visitor security pass (red lanyard).

If you are a lead official you must:

- i. Collect your visitors from reception promptly on arrival, sign them in and ensure you escort them to the exit barriers at the end of their visit;
- ii. Ensure that they visibly wear their visitor pass/lanyard at all times;
- iii. Escort your visitors at all times. For example, leaving your visitors alone in a coffee bar or allowing them to walk unescorted to and from open plan areas and toilet facilities is not permitted;
- iv. Do not take visitors into open plan areas, use a meeting room or communal facilities e.g. coffee bar.
- v. Ensure that visitors are aware that they must not take photographs on Welsh Government premises;
- vi. Inform Reception and Security if visitors will come into the building outside normal office hours.

8.4 Postal Mail

The Welsh Government mail system is for official business. All mail received at Welsh Government buildings must be opened only in Post Rooms or dedicated areas where staff are trained to deal with suspicious packages.

You must:

- i. Return any unopened mail to the Post Room/dedicated area;
- ii. Report any suspicious unopened mail to the Security Team 03000 253551 or the Local Facilities Manager;
- iii. Put the correct postage on any personal items that are sent via Royal Mail. Internal mail may not be used for personal items e.g. Christmas cards.
- iv. Send all business post via Welsh Government mail rooms. For example, you must not have business post directed to your home address or post items from home.

8.5 Opening of Personal Lockers

There may on occasion, be a business need for Local Facility Managers or their deputies to open a personal locker assigned to staff in their absence. Two staff members will always be present when a personal locker is opened by the Local Facility Manager/deputy using a master key.

8.6 Photography / Video

Taking photographs or video in or around Welsh Government premises can be problematic. Modern digital enhancement techniques mean that details in your photographs/video that can't be seen on your smart phone might be revealed at higher resolutions.

Photographs/video of individuals are also in scope of the Data Protection legislation. You must ensure that any photographs/video of colleagues (including Teams meeting records or screenshots) are not used for a different purpose than originally intended or uploaded to anywhere on the internet without the individual's permission.

You must:

- i. Ensure that any photograph/video that you take does not compromise the integrity of the workplace, buildings, information or any person(s) included in it;
- ii. Ensure that contractors whom you manage comply with this policy. If your contractors have a legitimate need to take photographs and you have given permission for them to do so, you must ensure that your contract management procedures include regular reviews to ensure the images are securely stored and disposed of;

- iii. Store photographs/video taken for work purposes in storage that has been allocated to you for that purpose and remove them as soon as practically possible from the camera/device on which they were taken;
- iv. Obtain permission from all of the individuals included before you take photographs/video.
- v. Obtain permission from all participants before recording a Teams video e.g. to re-use for training.

8.7 Vehicle Passes, Bicycles and Car Parks

You must:

- i. Comply with your local vehicle parking arrangements.

9.0 Personal Security

All employees undergo basic security checks before starting work for the Welsh Government and it is your responsibility to inform your HR Business Partner if you receive a formal (i.e. written) caution, are arrested, released on bail or convicted of a criminal offence during your employment.

9.1 Security Clearance (Vetting)

Vetting protects the integrity of the Welsh Government in terms of national security and possible physical threat against its staff and buildings. It also assesses whether individuals are suitable for specific posts which may involve contact with children or vulnerable adults. More information on vetting is available on the [intranet](#).

You must:

- i. Co-operate with the vetting process and complete security clearance forms honestly and in a timely manner;
- ii. Refrain from making any mention of your national security vetting security clearance on any social media or public platform e.g. LinkedIn;
- iii. Inform your HR Business Partner if you receive a formal (i.e. written) caution, are arrested, released on bail or convicted of a criminal offence;
- iv. Inform your HR Business Partner if your circumstances change, making you unsuitable for your post e.g. bankruptcy, change of nationality.

If you are a Line Manager you must:

- i. Make sure that all personnel e.g. new staff, contractors, student placements and secondees are vetted to the appropriate level before they start work;
- ii. Inform the Shared Service Centre if a specific post requires security clearance over and above the normal baseline check carried out for new staff;
- iii. Be aware of your staff's normal behaviour and report any unusual changes, security incidents or concerns to the [Chief Security Officer](#);
- iv. Ensure all Welsh Government equipment (e.g. passes, keys, IT equipment) is returned when someone you line manage leaves the organisation. Note there are separate policies which outline what should

be returned where someone is taking maternity, parental and adoptive leave.

10 WRA Section

In addition to the policy above, which applies to both Welsh Government and WRA, this section is solely for WRA staff.

- For references to iShare, read SharePoint. Store all information in SharePoint or other WRA authorised system, e.g. TMS, CRM or Dynamics365. If you are using your laptop offline, you must use your OneDrive which will sync with SharePoint when you are back online.
- For references to H: drive or iShare home folders, read OneDrive.
- For Information and Records Management Team, read Head of Information Governance.
- For IT Service Desk, read Digital Services Manager.
- For MyIT, read WRA Service Request.
- For HR Business Partner, read Head of HR.
- We do not usually allow Teams meetings to be recorded. Please contact your IAO if you want to record a Teams meeting.
- Access to the Zoom app is strictly controlled. Contact D&T if you need to access a Zoom event using the app.
- Log out of all WRA systems before logging off.
- When printing sensitive information, e.g. protected taxpayer information, WRA staff must use secure printing. If secure printing is not available, do not print sensitive information. Also, see the [Our Future Workplace](#) document on the WRA intranet for guidance on printing at home, which differs from the instructions at Annex C of this policy.
- WRA staff must only access or discuss protected taxpayer information when they can ensure their IT and telephony equipment cannot be overlooked, intercepted or eavesdropped by unauthorised persons. This should include being aware of the security of the network to which equipment is connected.
- Access to WRA secure areas/storage, e.g. investigation documentation, is restricted to authorised staff only. WRA staff and other relevant officials (as defined in section 17 of the Tax Collection and Management (Wales) Act 2016 (TCMA)) who have access to protected taxpayer information **must** sign a confidentiality agreement as set out in section 19 of the TCMA.
- The unauthorised disclosure of taxpayer information held by the Welsh Revenue Authority is a criminal offence under s17 of the TCMA.
- WRA staff should contact the WRA Head of Information Governance to ensure transfers of data outside the corporate network are lawful under data protection legislation and to ensure appropriate sharing agreements are in place. Staff should have a clear business purpose for gathering information regarding taxpayers. WRA staff must follow

the investigation guidance and processes and should not undertake any unauthorised research using the internet or social media as part of investigations into potential or actual taxpayers. The use of other channels such as social media to gather information for the purpose of our tax work are covered by a separate policy on intelligence gathering and surveillance. Please speak to the Head of Operations for more information

- Taking photographs/video that could comprise the security of protected taxpayer information is Gross Misconduct, unless it is strictly for legitimate work purposes, uses a WRA device and has been approved in writing by the line manager. You must be particularly careful to ensure no protected taxpayer information is captured if taking a photograph. Wrongful disclosure of protected taxpayer information is a criminal offence under s20 of the TCMA.

POLICY ENDS

Annex A – Examples of Misconduct and Gross Misconduct

Examples of Misconduct and Gross Misconduct

Protecting and Sharing Information

Misconduct

- i. Introducing material onto the Welsh Government network which infringes copyright. See: [Intellectual Property Rights \(sharepoint.com\)](#);
- ii. Disregarding standards of storage, handling, transmission or disposal of information. Examples include:
 - Storing information that is not connected to work (e.g. personal finances, personal correspondence, emails, images, music, video or games) on Welsh Government systems such as Outlook email folders, OneDrive, your iShare handy or My home folder. Note: if you are required to submit personal documents e.g. mortgage details to the Shared Service Centre then these may be emailed to your account, but the information must be deleted from your email (inbox and sent items) once you have passed it to the Shared Service Centre;
 - Emailing sensitive information outside the network or transferring it to other media (e.g. memory stick or online file sharing such as Dropbox or iShare Connect) so that you can work offline without the express permission of the relevant [Information Asset Owner](#) (IAO) or if your IAO is unavailable, your Line Manager. Note: your own personal documents related to work may be emailed to your home account e.g. payslip, P60, check-in notes, return to work interview notes. For avoidance of doubt, this extends to only your own personal information, you must not send anyone else's information outside the network e.g. check-ins for those in your team;
 - Deleting information in an attempt to avoid answering a request for information such as a data protection subject access request or a Freedom of Information request;
 - Accessing official or sensitive personal information (e.g. via iShare) that you do not have a legitimate business need to see;
 - Sending sensitive information outside the network via unencrypted email or to an insecure² email address (iShare Connect or #Encrypt should always be used when sending information to insecure email addresses);
 - Using Teams or any other program to transfer files externally of any kind.
 - Sharing sensitive information with external organisations without i) assessing the risk; and ii) obtaining prior approval to use an online tool as set out in the [Security Aspects of Using Collaborative Tools Policy](#);

- Taking official papers, keys or passes abroad (outside the United Kingdom) without the permission of your Line Manager. Before taking sensitive information abroad you require the approval of your Deputy Director and the Departmental Security Unit;
- Taking portable IT equipment overseas without first seeking authorisation from the [Departmental Security Unit](#). For more information refer to the [How do I... guide to Working and Travelling Overseas](#).
- Deliberately covering up or failing to report a data breach.

Gross Misconduct

- i. Trawling through paper or electronic records to access and misuse information in a way which causes reputational harm or loss to the Welsh Government or its employees;
- ii. Passing on information to others who are not authorised to see it (leaking). If you have concerns that you cannot report via your line management chain you must either follow the [Whistleblowing and Civil Service Code policy](#) or contact the [Chief Security Officer](#) in confidence;
- iii. Deleting information with the intention of preventing the Information Commissioner from viewing, or being provided with or directed to the information, document, equipment or material.

Protecting our IT (including Personal Use of Welsh Government IT)

Misconduct

- i. Moving or attempting to move fixed IT equipment (including telephones) yourself. Equipment moves must be managed by IT Services;
- ii. Introducing malware or causing disruption to normal IT service through reckless system use such as altering or disabling software (e.g. anti-virus software) that has been loaded onto your computer, smartphone or mobile device by IT Services;
- iii. Attempting to disable the synchronisation setting on laptops or other portable IT equipment which enables data to be automatically saved to the network after remote use;
- iv. Wilfully concealing the contents of a file or document by renaming it or by embedding it inside another file or document – e.g. pasting image files into a Word document;
- v. Forwarding non-work related images or other non-work related information to any email address (even if you have not opened the email);
- vi. Sending chain mail, unsolicited "spam" or indiscriminate communication;
- vii. Unauthorised installation of software or apps without authorisation from the IT Service Desk, no matter what media was used to install it;
- viii. Using another email provider (other than the approved program used by the Welsh Government to conduct official business) or adding another account (such as a personal account) to your smartphone or mobile device;

- ix. Attempting to attach any device to the Welsh Government network or IT equipment that has not been approved through the IT Service Desk or listed in Annex C of this document;
- x. Not taking reasonable care to secure Welsh Government hardcopy documents or IT equipment e.g. laptop, smartphone or mobile device). For example, if travelling by train do not leave the equipment/papers unattended on your seat while you visit the buffet carriage;
- xi. Lending or transferring personally allocated equipment such as laptops, smartphones and mobile devices to anyone else (e.g. colleague, friend or family member);
- xii. Allowing anyone else to access the IT network in advance of receiving their own username and password;
- xiii. Divulging your network password, laptop encryption password or PIN to anyone else (e.g. colleagues, visitors or family members) or demanding that a colleague share their own credentials with you;
- xiv. Dealing with personal business using Welsh Government IT equipment e.g. managing personal finances by storing or emailing spreadsheets, bank statements or insurance documents;
- xv. Using a Welsh Government email address or postal address for personal business, e.g. online shopping, booking holidays;
- xvi. Using Welsh Government equipment for personal reasons, e.g. to join a family quiz or exercise class;
- xvii. Using a personally owned IT device to undertake social media activity on behalf of the Welsh Government;
- xviii. Changing the Welsh Government email address associated with a social media account to a non-Welsh Government email address;
- xix. Sharing social media password details with third parties. Third parties are not to have any password details of any Welsh Government social media account;
- xx. Failing to apply two factor authentication for all Welsh Government social media accounts where it is available (note: this does not apply to Welsh Government social media accounts that are accessed from Welsh Government devices and Hootsuite as these provide an alternative control);
- xxi. Use your Welsh Government device to make personal/social calls to friends and family (except in an emergency e.g. caring responsibilities). Social calls should only be made from your personal device.

Gross Misconduct

- i. Downloading, accessing, emailing or otherwise introducing material into the Welsh Government that causes offence to colleagues (e.g. sexually explicit/obscene media) or contravenes Welsh Government policies such as Equal Opportunities or Dignity at Work;
- ii. Using Welsh Government systems to commit fraud or other illegal/criminal activity;
- iii. Using Welsh Government IT systems or contact details to run your own business or undertake any other activity that is associated with profit (either personal or business-related);
- iv. Sending email or other electronic messages which might interfere with your official duties or bring the Welsh Government into disrepute;

- v. Accessing web sites, chatrooms and using social media (even in your own time or from devices not owned by Welsh Government) in a way which might interfere with your official duties or bring the Welsh Government into disrepute;
- vi. Falsifying records, such as logs, email or other electronic transmission;
- vii. Deliberately introducing software with the intention of causing damage to Welsh Government IT systems;
- viii. Hacking (attempting to bypass or subvert system security controls) or otherwise deliberately obtaining unauthorised access to corporate systems or other user accounts. This includes attempts to remove laptop casings or any other component e.g. hard disk;
- ix. Making publicly available any information which incites, encourages or enables others to gain unauthorised access to the Welsh Government IT systems;
- x. Logging on as another user or accessing any IT systems that you have not been given permission to access.
- xi. Failing to secure classified information (see the [Handling SECRET Information Policy](#)).

Working Securely Away from the Office

Misconduct

- i. Using your own IT equipment for processing or storing Welsh Government information. Note: exceptions include an approved personal printer, using a personal phone to 'twin' with the telephony system or use of the Microsoft Authenticator app;
- ii. Taking sensitive material and/or keys or using Welsh Government equipment abroad without prior authorisation;
- iii. Failing to lock information and IT equipment in a car boot out of sight; or keeping such items in an unattended vehicle overnight;
- iv. Taking OFFICIAL-SENSITIVE hard copy information out of the office without the approval of your IAO (or Line Manager if your IAO is unavailable);
- v. Printing OFFICIAL-SENSITIVE information at home without the approval of your IAO (or Line Manager if your IAO is unavailable);
- vi. Attaching unauthorised personal devices to your laptop.

Maintaining Physical Security

Misconduct

- i. Disregard of, or non-compliance with, appropriate instructions from security staff;
- ii. Failing to adequately supervise visitors to Welsh Government buildings (where you are the lead official). Examples include:
 - Allowing visitors to walk around Welsh Government premises unescorted;
 - Allowing visitors to make their own way out of Welsh Government premises;

- Allowing visitors to take photographs on Welsh Government premises;
- iii. Signing in anyone who should be security cleared (e.g. contractor, secondee) as a visitor while they are awaiting security clearance unless a written dispensation has been received from the Corporate Shared Service Centre;
- iv. Using the internal mail service for personal use or arranging for personal deliveries to a Welsh Government office;
- v. Taking photographs/video in a way that could comprise the security of Welsh Government premises or lead to a breach of the Data Protection legislation. Examples include:
 - Taking photographs/video of computer screens or official papers without the express permission of your Information Asset Owner or line manager;
 - Uploading any photographs/video that you have taken for work purposes inside Welsh Government premises to the internet (e.g. social media sites) without the express permission of your Line Manager;
 - Using any photographs/video of colleagues for a different purpose than originally intended or uploading such items to social media sites without their permission.

Gross Misconduct

- i. Theft of equipment, data or other property belonging to the Welsh Government, including personal property stolen from Welsh Government buildings;
- ii. Allowing someone else to use your building or car parking pass, or asking someone else for use of theirs;
- iii. Unauthorised access to restricted areas (e.g. by bringing people into the work areas who are not staff members or attending the office on official business).

Personnel Security (Vetting)

Misconduct

Stating your clearance level on a public forum or social media e.g. LinkedIn.

Gross Misconduct

Failing to disclose an arrest, charge or conviction for criminal offences while undergoing vetting.

Annex B – Inspectors

The following rules apply to Inspectors in HIW and CIW.

- i. Where possible, paperwork and IT devices must be left in a secure location e.g. locked office. The laptop must always be shut down so that you enter your BitLocker encryption PIN when you next login.
- ii. There will be times during inspections when a secure location to store IT devices and paperwork is not available. In these instances, the **laptop** may be left in a location that would not normally be considered safe provided it is the only option available. The chosen location must be as discrete as possible. A laptop must never be left unattended if the hard disk encryption has not been activated.
- iii. This exemption only applies to **laptops**. If a secure location is unavailable, then other mobile IT equipment (work phone/iPad etc) and hardcopy paperwork must be carried by the Inspector.
- iv. As a general rule when making a reasoned decision to leave a laptop in an insecure location, the Inspector is expected to apply the same level of care to Welsh Government IT equipment as they would their own personal IT device or handbag/wallet.

Annex C – What personal devices can I connect to my laptop?

You must not attach ANY device to the corporate network or IT equipment that has not been approved through the IT Service Desk. This includes charging personal mobile phones or tablets via the USB port on your laptop or docking station.

Removable devices, such as USB devices used for work related purposes, must be obtained through centrally agreed arrangements. Only Bluetooth headsets supporting Bluetooth 5.0 or above are permitted.



Monitors / TVs – either wired or wireless



USB or Bluetooth mice, USB or Bluetooth keyboards



Wired USB or Bluetooth Headsets - Only wired USB or Bluetooth headsets that support Bluetooth 5.0 or above are permitted. You must ensure that you have correctly paired the headsets directly to your laptop prior to use. If uncertain about pairing to the correct device, then you must remove and restart the pairing. IT Services are unable to offer support in connecting personally owned headsets, so please refer to your manufacturer's guidance if you experience any issues.

Please note the exception that wireless headsets meeting DECT standards issued by IT Services as part of a reasonable adjustment are permitted.



External cameras



Printers: but ONLY if:

- Your printer is Mopria certified; **and**
- Your printer is connected to your laptop by a USB cable; **and**
- You have a personally owned shredder that meets the P-4 standard (i.e. where the shredded particles are less than 6mm in width **and** the overall area is less than 160mm²) to shred OFFICIAL-SENSITIVE or personal information and mix the particles with normal household waste.

Note: you **cannot** claim reimbursement for either the printer/shredder or any consumable items e.g. paper, ink.

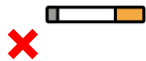
What personal devices can't I connect to my laptop?



Wifi Headsets (only wired USB and Bluetooth headsets are permitted).



USB / Bluetooth Smart Speakers including digital assistants like Amazon Echo and Google Nest.



Electric cigarettes / Vapes: do not connect devices to your laptop to charge them. Use a 3 pin socket instead.



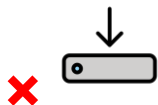
USB novelty items such as Christmas lights, desk fans, cup warmers.



Jigglers: These devices connect to your laptop and are designed to keep your screen active by randomly moving your mouse. They can also give the appearance that you are active on your laptop when you aren't (e.g. Teams status).



Mobile phone: Do not charge your personal devices e.g. phone or tablet from your work laptop or docking station.



Memory sticks / hard drives: While you have read-only access on your laptop, under no circumstance should you connect memory sticks / hard drives from unknown sources (e.g. found in the street or from trade shows) as these could be malicious. USB read access is only allowed for memory sticks / hard drives that have been approved for business use.

Annex D – Authorised Lanyards

Staff Lanyard



Contractor Lanyard



Welsh Learner Staff
Lanyard



Welsh Speaker Staff
Lanyard



Visitor Lanyard



Conference Visitor Lanyard



Yr Hafod Visitor Lanyard



Tenant Lanyard



Welsh Speaker Tenant
Lanyard



NRW Tenant Lanyard (due
to be phased out with
standard tenant lanyard)

