Estyn | Dros ddysgwyr, dros Gymru
For learners, for Wales

IT usage policy

Information sheet

Information box

For further advice contact: Information Technology Cyber Security Officer (ITCSO)

Date of publication: December 2025

Version: 5.0

Version control

Document version	Author	Date of issue	Changes made
1.0	Information Technology Cyber Security Officer	July 2021	New policy
2.0	Strategic Programmes Director	October 2024 Approved by SMG XXXXX	Updates to uses of MS Teams Changes to setting password rules to align with National Cyber Security Centre Strengthened wording around information governance Encourage users to use SharePoint and OneDrive, USB devices in exceptional circumstances only Added narrative around emails going into quarantine Update hyperlinks to other policies cited in this document Guidance on use of AI hyperlinked Guidance on insurance for staff working from home Guidance on use of personal numbers in a business capacity

Equality Impact Assessment

A business rationale assessment has been carried out and this policy contributes to Estyn's strategic objectives and delivery principles.

In accordance with Estyn's Equality Impact Assessment, an initial screening impact assessment has been carried out and this policy is not deemed to adversely impact on the grounds of the nine protected characteristics as laid out by the Equality Act 2010.

The following definitions apply within this policy:

MUST – This word, or the terms "required" or "shall", mean that the definition is an absolute requirement.
MUST NOT – This phrase, or the phrase "shall not", means that the definition is an absolute prohibition.
SHOULD – This word, or the adjective "recommended", mean that there may exist valid reasons in particular circumstances to ignore this behaviour/instruction/action, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT – This phrase, or the phrase "not recommended" mean that there may exist valid reasons in particular circumstances when the particular behaviour/instruction/action is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY – This word, or the adjective "optional," mean that an action is truly discretionary.

Contents

1 Introduction

Our information and communication technology network, equipment and telephones (hereafter referred to as the 'IT systems') are provided for staff use only. This policy is designed to make sure that the use of our IT systems is efficient and secure and does not expose us to major business or legal risks.

Each user of our IT systems is responsible for helping to prevent information security breaches. Users are responsible for reading the rules in this document and should be aware that by logging on to our corporate network they agree to be bound by the terms of these rules.

Our IT team should be your first port of call for all enquiries about our IT systems; message helpdesk ITsupport@estyn.gov.wales or phone if you are unable to access your email. If the internal IT team are unable to deal with your enquiry they will liaise with external support providers to find a solution.

This policy explains the rules about acceptable use of our IT systems. The rules apply to all staff and to consultants and contractors who are given access to our IT systems; contracts will reflect this.

Staff are allowed some limited personal use of our IT systems as set out in Section 5 of this policy.

These rules will be reviewed and updated regularly. Any changes to the rules will be communicated to staff on SharePoint and our other corporate communication channels.

This policy is part of a group of policies relating to information governance. Other documents related to this policy include:

- The Human Rights Act, 1998
- The Computer Misuse Act, 1990 (and Part 5 of the Police and Justice Act 2006)
- The Data Protection Act, 2018
- The Regulation of Investigatory Powers Act, 2000
- The Freedom of Information Act, 2000 The Official Secrets Act, 1989
- The Investigatory Power Act 2016
- General Data Protection Regulation (GDPR) 2016
- The Fraud Act 2006
- Privacy and Electronic Communications Regulations (PECR) 2003
- Children's Code (Age-Appropriate Design Code) 2020
- Copyright, Designs and Patents Act 1988

Any information stored on or shared using our IT systems is not private and may be checked (read, listened to or copied), without notice, for the following purposes:

- quality control and staff training
- maintaining compliance with practices or procedures set out in law
- protecting the interests of Estyn
- preventing unauthorised use of IT systems
- preventing inappropriate or offensive media being stored on or shared using the IT systems
- assisting with any investigation or action proposed by lawfully authorised investigatory or regulatory bodies (e.g. Police)
- complying with access to information requests under the General Data Protection Regulation and the Freedom of Information Act (requests for information from external parties and staff)

We also reserve the right to make and keep copies of all information (including but not limited to telephone calls, emails and data logs of use of IT systems and equipment) for the purposes set out above. The information may be used in disciplinary proceedings.

2 Health and safety

Advice on workstation assessment and any issues regarding accessibility is available from Estyn's Health and Safety Officer and the Human Resources team.

3 Care of IT equipment and data

All of our equipment is logged on our Asset management system and allocated to individuals. You are responsible for taking care of the IT equipment issued to you and you must not pass this equipment on to other individuals. As part of our internal audit procedure, you may be required to the need to respond to requests for confirmation that assets are still in the individual possession in a timely manner and upon request, the need to provide physical evidence of possession (i.e. via a photograph).

To avoid potential loss of data you should save your work regularly and shut down your computer before you finish work for the day as this is good for security reasons and for your own well-being. It is also recommended that you switch off the power source when not using your laptop as this will help prevent battery degradation.

All information must be saved to OneDrive and SharePoint. In exceptional circumstances, you may use devices such as USB. You must take extra care if you need to use removable media (e.g. USB sticks). These items are especially prone to viruses and potential loss of data – further advice is provided in Section 12 of this policy.

If you lose or damage equipment that is allocated to you (including removable media), you must report it to the Information Technology Security Officer (ITCSO) and your line manager straight away. You may be charged for negligent loss or damage to equipment.

You should avoid:

- eating or drinking over a computer
- trailing wires where people might trip over them

You must not attempt hardware repairs, for example do not try to open computer or telephone equipment casings.

Data stored on your computer, for example within Desktop, Documents and Pictures will be backed up to your OneDrive however users should note that all other locations on your PC will not be backed up. These areas should only be used for storing files temporarily and you should clean out these files regularly.

You must lock your screen when you leave your computer unattended, even if you only leave it for a short time (hold CTRL-ALT-DELETE and click ‘Lock’ or hold the Windows key and press L).

You can set your auto screen lock timings to whatever duration you like, including disabling the auto screen lock. If you disable the auto screen lock, you shouldn’t leave your computer unattended at any time.

If you believe that someone has accessed your network account without your permission, you must inform your line manager and the ITCSO immediately.

When you access or process sensitive information, you must take all reasonable precautions to make sure that other people cannot view your screen – remember that your screen may be more easily overlooked than a sheet of paper on your desk. Users can request privacy screens by contacting the IT helpdesk. 3.12 Please be mindful of the extremely sensitive data we hold and use. It is your responsibility to ensure active steps are taken to ensure confidentiality is preserved. The sharing of confidential information is strictly forbidden, and any breach would be a serious disciplinary matter.

If you are contacted by telephone, just as you should in your personal life, make sure that you are aware of the identity of the caller before discussing or sharing sensitive

information. Please be mindful of the extremely sensitive data we hold and use. It is your responsibility to ensure active steps are taken to ensure confidentiality is preserved. The sharing of confidential information is strictly forbidden, and any breach would be a serious disciplinary matter.

In exceptional circumstances, if you need to hold sensitive information on removable media (e.g. USB memory stick) then you must store it securely when it's not in use. Personal data should only be stored on an encrypted device. Any information that you store on removable media should be deleted once you no longer need it, or when you have transferred it to permanent media (for example SharePoint).

You should never divulge information that could compromise the security of our systems to third parties without verifying their identity and why they need the information. Ask yourself: does this person need to know this to do their job? This includes details of our IT systems, software applications, or details of your network username.

4 Home insurance requirements

Employees who work from home must ensure that their home insurance provider is made aware that occasional administrative work is carried out from your property. This is to ensure that home insurance cover remains valid and appropriate.

Staff should declare to their home insurer that their role may involve working from home using IT equipment provided by Estyn, for tasks such as document editing, communications, and data processing. This declaration is typically considered low risk and does not usually impact premiums, but it is essential to inform the insurer to avoid any issues in the event of a claim.

Estyn does not accept liability for personal property damaged during work activity at home unless this was caused by a fault in Estyn-issued equipment. Employees are also responsible for ensuring that any Estyn-issued equipment used at home is kept securely and safely in accordance with this policy.

5 Systems security

Users access our IT systems with a unique username, and each account is password protected. Where Multi Factor Authentication(MFA) is an option the it should be used as it provides an additional level of security. You must not log on as another user or access any

IT systems that you have not been authorised to access unless you are following the instructions of our IT helpdesk.

You are responsible for all network activity on your account while you are logged in to the system. You must not let anyone else use your username, password or PIN. If you need to share your login details for technical support purposes, you should change your password as soon as possible afterwards.

You should only log on to your account from one computer at a time. If you need to log on to your account from another computer at the same time (for example when you're presenting information at a meeting away from your desk) make sure that any other computer, you are logged on to has been locked.

You and your line manager are responsible for making sure that any important work-related information including important emails, is stored in Estyn's intranet, especially if you are leaving Estyn. Your manager will make sure that the information we retain after you leave is managed in line with GDPR requirements.

You should use passwords that are not familiar and easy to guess. For example, do not include family names, place names, or any other information that people know about you. Estyn sets the password rules – when changing your password, it must be a minimum length of 12 characters, and must contain three of the following four elements:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- base 10 digits (0 through 9)
- non-alphabetic characters (for example, !, $, #, %)

You can only try ten times to type in your password correctly before your account is automatically locked for fifteen minutes. You will not be able reuse old passwords.

If you believe that someone else knows your password or PIN, you must change it immediately.

If you have forgotten your password, please contact the IT team so it can be reset.

Only software or systems approved by our ITCSO may be installed on our equipment. You should email requests to install new software to ITsupport@estyn.gov.wales who will review your request.

You must only connect non-Estyn equipment or removable media to Estyn IT systems under the guidance and advice of a member of the IT Team, this is to assess and manage security risks, for example virus or malware contamination.

You should report any security weaknesses you see or suspect, or threats to our systems, to the IT team and/or the ITCSO, Ben Thomas.

Phishing emails are now commonplace including phishing style text messages. Forward any suspicious emails to our IT team. Spoof emails are becoming more prominent. These are emails that look as if they are coming from someone you know back are in fact a Phishing email. Always check the full email address.

Emails deemed risky will be placed into quarantine. You are now able to manage quarantined emails. If you receive an email from "quarantine@messaging.microsoft.com" with the title of "Microsoft 365 security: You have messages in quarantine" this means that a low risk email has been placed in quarantine and also mean that users can release it themselves.

If someone outside the organisation tells you that a computer virus may have entered the Estyn network, you must inform the IT team straight away. Don't send out a warning to other staff; email the IT Service Desk and let them send out any necessary warnings.

If you receive a suspicious email with an attachment or link, don't open anything; forward the email to the IT team for checking.

If there is a virus outbreak on our systems, users must follow the instructions given by the ITCSO or IT team.

You must take responsibility for protecting the assets assigned to you by making all reasonable efforts to make sure that you minimise all opportunities for theft or loss of information and equipment. For example:

- On laptops, tablets and mobile phones: you must use all available security protection to prevent unauthorised access, e.g. passwords, keypad locking or PIN codes.
- If working in an area that is accessible by others, ensure that you lock your screen if you leave your equipment unattended. You should store IT equipment in a secure location when not in use – preferably, in lockable desk drawers or cupboards where they're available.
- Do not leave IT equipment unattended when travelling.
- Whenever possible, carry your portable equipment as hand luggage.
- If you need to leave your equipment in a vehicle, make sure that it is locked away and out of sight. However, we strongly recommend that you don't leave equipment in vehicles overnight.
- Don't create temptation – be discrete when carrying or using equipment in a public setting and be aware of being overlooked or overheard at all times.

Please note that if your laptop is lost or stolen, it will be wiped remotely, and anything not saved on our network will be lost. See para. 3.7 on how information is stored and backed up.

6 Personal use of Estyn IT systems

All equipment is provided for the purpose of undertaking Estyn business.

However, we do understand that personal communications are sometimes necessary during the working day, and you are allowed reasonable use, i.e. where:

- it is restricted to non-working time and does not get in the way of your work, except in emergencies
- it will not embarrass us or our staff, or cause any reputational damage (this includes comments or content on social media, see our social media policy for more details)
- it does not affect the performance of the IT systems
- there is no copyright infringement or other unlawful activity
- it is not for any personal or business profit with any external organisation

Personal use of official IT systems is at management discretion and is not an automatic right. Generally, you should not use equipment which is connected to our network to log on to any personal email due to the increased security risk. When you're on inspection or any other 'remote' service, we recognise that you might want to catch up on personal email – this is considered acceptable use. However, you should be careful not to open any suspicious emails or attachments which might contain viruses.

You must make sure that all data complies with legal requirements. For example, you are responsible for making sure that media files do not infringe copyright.

Any personal or non-work-related files stored on any work drive are stored at your own risk.

Any non-work-related files that are found on our IT systems may be deleted without notice.

7 Use of personal mobile numbers for work purposes

Estyn devices are the primary method. Where issued, staff should use Estyn provided mobile phones or approved communication tools (e.g. Microsoft Teams, official landlines) for all business communications.

Personal numbers only when necessary. Sharing personal numbers is voluntary and only when operationally necessary—e.g. unexpected inspection calls. Use of personal devices remains a staff choice and shouldn't be expected. Staff should consider carefully whether it would be appropriate to share their personal number with colleagues or educational professionals they meet within a work context. If you are sharing your number for the purposes of Estyn business, you should normally share your Estyn mobile number and e-mail.

Loss or theft any device that an Estyn account has been logged into must be reported immediately to the IT Service Desk. Users are responsible for costs, maintenance and insurance of their personal devices. Estyn does not reimburse charges or support non-corporate apps.
Breaches of this policy may result in disciplinary action.
Regular usage triggers official device offer. If you're expected to regularly use your personal mobile for work, you should discuss obtaining an Estyn issued device with your line manager.

8 Use of email and messaging platforms (official and personal)

All emails that are sent from or to the Estyn network are scanned for viruses, spam and inappropriate images. It is not easy to define what constitutes an inappropriate image, but this could include any picture with full or partial nudity, pictures that show violence or discrimination towards others, or images which could be seen as inciting hatred towards any group or individual. This includes all protected characteristics as outlined in the Equality Act 2010. Remember that images that are seen by some people as funny can cause offence to others.

The illusion of "privacy". Be aware that, between the writer of an email, Instant Message, etc. and its recipient(s) a message may be recorded several times. Copies of messages can be retrieved and read by people other than the intended recipients (for example for subject access requests under the Data Protection Act or Freedom of Information Act).

Ethical issues. It is important that nothing is contained within an email or message which could potentially be considered as offensive to the recipient or any other person.

The potential legal liability. Email and messages carry legal risks (called 'vicarious liability') for the user and Estyn as a result of the accidental or deliberate infringement of any laws. You may inadvertently commit an offence under one or several of the acts listed in 1.7.

If you have any queries about the content of an email that you've received or that you're about to send, you must consult either your line manager, Human Resources or the ITCSO. If in doubt, don't send the email.

You should not use your Estyn email account to send non-work-related messages, particularly to recipients outside of Estyn.

All staff must use bilingual out-of-office messages and auto-signatures. You should only use text in your signature that follows the Estyn template. The Communications Team may also ask you to temporarily include campaign-specific content in your signature.

When you use our email system (Outlook), you must not automatically forward emails from your Estyn email account to another email account. If you do this, you could accidentally send protectively marked information out of the network, which would be a breach of data protection. Please refer to the Information Assurance Policy. for how to categorise email subjects when sending sensitive information.

For days that you are not working you should set up an out of office message using the guidance that is sent out periodically. If you are going to be away for an extended period (e.g. sick leave), your line manager can ask the IT Service Desk to reset your message. Your out-of-office message and auto-signature must only be used to give your work contact details, or those of colleagues to be contacted in your absence. You shouldn't include your personal contact details.

Use of Microsoft Teams

Microsoft Teams is now one of the primary methods of business communication. It is important to understand your responsibilities in using this platform.

You should ensure that all conversations within Microsoft Teams are work-related and do not insult, demean, bully, harass or discriminate against another person or group of people. Team's messages can be recovered by the IT department, and you should refrain from posting any message which could be construed as offensive. Microsoft Teams messages, including chats and channel conversations, are subject to Freedom of Information Act (FOIA) requests and General Data Protection Regulation (GDPR) Subject Access Requests (SAR), meaning they may be disclosed in responses to requests for information.

Teams group chats are a convenient way to keep in touch with your team whilst working remotely, and we encourage their use for work-related purposes. However, you should remember that Teams notification messages can also be disruptive, so use the platform wisely and do not 'spam' group members with multiple unnecessary messages. Teams conversations are kept for 3 months only.

When using your device to present, please ensure your Teams notifications have been switched off.

9 Use of the internet and mobile phones

We provide internet access for undertaking our business. You may also use our internet connection for personal reasons, if this does not interfere with your work or embarrass Estyn or its staff. When using your own personal device at the Estyn office please use the EstynGuest wireless network.

Estyn accepts no liability for any loss or damage suffered by any user arising from personal use of the internet.

You must not use work devices to access websites or chatrooms that are offensive or inappropriate to the workplace. We automatically restrict access to certain categories of website. However, even if access to a site hasn't been restricted, you shouldn't assume that the site is appropriate or approved. If you accidentally access an offensive website or chat, you should close the window or tab straight away and tell your line manager and the ITCSO about the incident.

If you need access to a blocked site for legitimate work-related reasons, you should request access from the ITCSO. You should also explain why access is necessary; you might be asked to write a business case if it's appropriate.

You must not attempt to download software from the internet as the system will prevent you from installing software without permission from an administrator. If you are prompted to reboot your machine following an update you must do so as soon as possible as these may include important security updates. To reboot your machine, select the option to "restart" under "power" in the "start" menu (Windows logo) in the bottom left corner of your screen.

Mobile phones are often a target for thieves, so you should always use and store them discreetly, for example don't leave them unattended in jacket pockets, handbags, etc., in a publicly accessible space.

You must use all the security methods available to you to prevent unauthorised use or theft, for example keypad locking codes, pin-codes and biometric access.

If your work mobile is stolen or lost, you are responsible for contacting the IT Team immediately. They will arrange a call with the network provider and a remote 'data wipe' as soon as possible. You must also inform the police and get a reference number (a crime

number or lost property number). You may be held responsible for paying the full cost of a replacement handset, depending on the circumstances of the loss.

If you are driving and using a mobile phone, you must adhere to our Policy for driving as part of official duties. It is unsafe and illegal to use a hand-held mobile phone whilst driving a vehicle, apart from using e.g. google maps. If you are fined for doing this while you're on business activity, you are responsible for paying the fine. We recommend that you don't use a mobile phone while you're driving; switch off your phone, use a message service, or let a passenger make or answer a call.

Mobile phones can be disruptive to others while you're working. You should turn off your personal mobile phone or set it to 'silent' or low volume ringtone during working hours.

10 Use of Artificial Intelligence

Staff must ensure they comply with our guidance on AI: Artificial Intelligence - Estyn Any concerns or questions should be communicated via itsupport@estyn.gov.wales

11 Delegated working

We recognise that there are times when you might need to access a colleague's calendar or mailbox, either on an ongoing basis (for example if you're an Executive Assistant), or just occasionally to cover periods of staff absence.

You must not share your personal login details with others; there are IT facilities that let you access calendars and mailboxes without having to share login information.

You may request ongoing, delegated access to a colleague's calendar and mailbox through your line manager; they will send a support request to the IT Support.

If you need to allow colleagues to monitor your incoming email or calendar entries while you're out of the office, you can set your Outlook permissions to allow this. For more information on setting permissions, contact the IT Support.

12 Remote support

There may be times when the Estyn IT Team or IT service provider will need to access your IT equipment remotely. This is to ensure your equipment is up to date and to perform maintenance.

Permission will always be sought when accessing your IT equipment. To speed up the process this may be verbally whilst on a call with you or this could be at an agreed time confirmed by a calendar entry.

You should note that our IT team have Administrator privileges on Estyn equipment meaning they will have access to all software, and storage areas such as your c: drive. Remember personal files are held at your own risk and will be visible to our IT team.

On certain occasions (such as maintenance or remote repair) the IT Team may need access to hardware (such as webcams) connected to equipment. It is your responsibility to ensure any personal space you do not wish to be seen is out of the field of view of such equipment.

13 Travelling overseas

Estyn IT equipment should only be taken overseas when travelling on Estyn business. Requests to work remotely in locations outside of the UK should initially be referred to your line manager for approval following a risk assessment.

Do not take any information marked ‘protected’ or commercially sensitive information with you unless it is essential for the purposes of your visit. Before you leave you must tell the ITCSO if you need to take this type of information with you. The ITCSO will be able to offer advice on how to protect the material when you’re travelling, and during your stay.

Airports

You must comply with all port of entry instructions for IT equipment, even if it would be in breach of our IT Security and Usage Policy. For example, if an immigration official tells you to start up your computer and divulge your password then you should do so. However, you should change your password and inform the ITCSO of the incident as soon as you can.

When you go through airport scanners, try to avoid a situation where your laptop bag emerges from the luggage scanner before you have walked through the security checks. (There have been cases where thieves have taken laptop bags from the conveyor belt before the owner has been able to pick the equipment up).

You may be asked to start up your equipment at airline security checks. Make sure that you have a full battery before you start your journey. If your laptop doesn’t start, it could be confiscated.

Normally, all IT equipment must be carried as hand luggage. However during a time of heightened airport security it may not be possible to take any equipment through as hand luggage and in this case, you will need to put your IT equipment in the hold.

14 Handling personal data

You must not take devices that store personal data (i.e. that could cause damage or distress to individuals if it's lost) outside our offices unless they are **encrypted** and/or capable of having data wiped remotely. Most colleagues will not need access to personal data for business reasons. Personal data must only be stored either on Estyn's network or in exceptional circumstances on an encrypted device.

Under the Data Protection Act and GDPR, **all personal data** should be handled in a secure manner. You must take extra care if you take any personal data outside our premises on any device.

Our policy on personal data handling is explained below:

Level of sensitivity	**Level of protection**
Personal data	May not be removed from secure storage (digital or physical for paper) without approval and should be stored on encrypted device
Sensitive data, e.g. draft inspection reports	May be removed from Estyn secure storage. Preferably, should be stored on encrypted device but, for practical reasons, a non-encrypted device (e.g. USB stick) may be used with extra care taken to avoid loss
Data which if lost is unlikely to cause damage or distress – e.g. information is already in the public domain or would be released under a Freedom of Information request	May be removed from Estyn secure storage without encryption

Please contact the ITCSO if you are not sure about how you should handle personal data.

If you use an unencrypted laptop, for example for giving a presentation, then you should save the data to a memory stick. The presentation should either be opened and shown from the file on the stick or transferred to the device's desktop and opened from there.

When you've finished using the file, you must delete it and empty the recycling bin. This is standard practice when you use unencrypted equipment to avoid any risk of data leakage.

All information, including records held electronically, must be classified in accordance with the UK Government's Protective Marking Scheme.

For more information on how and when to apply protective markings, read our Information Assurance Policy.

15 Removable media

In exceptional circumstance, if you need a removable media device for business purposes, like a USB data stick, you should request these from the IT helpdesk Services team. There are risks associated with using USB sticks not provided by Estyn, for example free USB sticks given at events.

Please seek advice from the IT team, if you wish to attach any device to IT equipment issued by Estyn.

Data held on removable media storage devices is vulnerable to loss. These devices are also a ready source of malware propagation. You should assess any risks associated with the transfer of data onto our systems via removable media. If you're not sure, contact the ITCSO.

When using your mobile or Bluetooth devices on any Estyn equipment, please be mindful that there are increased risks of interception.

16 Use of Cloud based software

This section outlines the rules and responsibilities for the use of cloud-based software within the organisation. Cloud services offer flexibility, scalability, and enhanced security when used appropriately. This policy ensures that such services are used in a secure, compliant, and efficient manner.

Approved Cloud Services

Only cloud-based software that has been formally approved by the IT Security Officer (ITCSO) may be used. Approved platforms include, but are not limited to:

- Microsoft Office 365

- SharePoint and OneDrive
- PowerBI
- SAP Concur
- ClickTravel
- Adobe Creative Cloud
- PeopleHR
- EventsForce
- Sage Intacct

Any new cloud service must undergo a formal risk assessment and approval process before deployment.

Data Storage and Access

All organisational data must either be stored in approved cloud environments (e.g., OneDrive, SharePoint) or within storage provided as part of a cloud-based software solution. Sensitive data must not be stored in personal cloud accounts or unapproved platforms. Wherever possible, access to cloud services should use Single Sign On (SSO). In the absence of SSO, access to cloud services must be restricted to authorised users only, using secure login credentials and multi-factor authentication where available.

Security and Compliance

Any integration with third-party systems must be reviewed to ensure secure data exchange and minimal exposure to cyber threats. Where possible, cloud services should be restricted to be use on Estyn devices only. Full consideration should be given to the sensitivity of the data being secured when deciding whether to restrict access to Estyn devices.

User Responsibilities

Users are responsible for safeguarding their login credentials and reporting any suspicious activity. Users must not attempt to bypass security controls or use cloud services for unauthorised purposes.

16 Breaches of the IT usage policy

Breaching this policy could result in disciplinary action and possible dismissal. Some Breaches may also lead to legal action against you under the acts listed in 1.7.

Potential breaches of this policy which come to the attention of management will be investigated by the Human Resources team and the ITCSO. The Human Resources team is

responsible for taking the lead in any disciplinary proceedings arising from a breach of these rules by our staff. Where we decide that disciplinary action is necessary, we will undertake formal action. Our staff should refer to the Discipline Policy and the 'formal action' section of the Discipline Procedures.

We will only investigate an allegation of a breach of this policy if there is reasonable suspicion that a breach has occurred. The investigation may involve actions such as accessing emails or other information stored on or communicated using our IT systems. This may include consideration of a user's internet use.

The user will be informed at an appropriate time that such steps have been taken in relation to them, with an explanation of the reasons why those steps were taken. Once an investigation has been completed, if appropriate, the investigating officers will destroy copies of any evidence they have collected.

We will co-operate fully with the police or government officials of an appropriate level in any investigation relating to unlawful activities conducted using our IT equipment or systems. If the investigation uncovers material that could be considered as an instance of misconduct or gross misconduct, we will follow the appropriate disciplinary procedures.

In all cases of illegal acts, we will notify the police. We may disclose evidence to the police where there is reasonable suspicion of criminal activity.

You must inform the IT Service Desk and the ITCSO if an IT security breach is suspected or detected. You should also speak to your line manager or the Human Resources team, or you may speak to a designated officer under our Whistleblowing policy.

Possible offences

Breaches of this policy can result in misconduct investigations. The result of a proven case can vary from an informal or formal warning to dismissal. However, we will consider each case on its own merits. If the allegation of a breach is proven, we would decide on an appropriate penalty, based on:

- the circumstances of the case
- the level of seriousness of the offence (minor, serious or gross misconduct)

Misconduct

This list of activities gives examples of conduct considered to breach acceptable IT use, though it is not exhaustive. These examples would normally lead to disciplinary action:

- introducing malware or causing disruption to normal IT service through reckless system use

- sharing your password or demanding a colleague to share their password with you
- introducing material which infringes copyright
- ignoring standards of storage, transmission or disposal of information, for example storing personal movies, inappropriate graphics or image files, animations or games
- sending communications which might damage Estyn's reputation
- excessive personal use of email or the internet at the expense of the interests of the organisation
- unauthorised installation of software, whether it has been downloaded from the internet or installed from physical media
- sending chain email, unsolicited spam or indiscriminate communication
- canvassing, lobbying or propagation of personal opinions such as political or religious beliefs
- making false claims or denials regarding the use of our systems
- misuse of social media (see our Social Media Policy and Guidelines for more information)

Gross misconduct

Gross misconduct is a deliberate activity which constitutes a major breach of conduct in the use of IT, which brings Estyn into disrepute and/or which makes any further working relationship or trust between us and the employee impossible. Examples include:

- downloading, accessing, emailing or otherwise introducing material that causes offence to colleagues, or which contravenes our policies (for example the Equal Opportunities Policy)
- using our systems to commit fraud or other illegal or criminal activity
- falsifying records, such as logs, emails or other electronic transmission
- downloading, accessing or otherwise deliberately introducing sexually explicit or obscene media into Estyn
- introducing software to the system intending to cause damage to our systems
- using email or communication methods to circulate deliberately threatening material
- hacking (attempting to bypass or subvert system security controls) or otherwise deliberately obtaining unauthorised access to our systems or other user accounts
- theft of equipment, data or other property belonging to us, including personal property stolen from our offices
- logging onto our systems as another user or accessing any IT systems that you have not been given permission to access
- serious misuse of social media (see our Social Media Policy and Guidelines for more details)

17 Linked Information Governance Policies

Estyn information governance framework sets out our key information governance policies, all of which can be found on our website under corporate polices.

Glossary

Application (App)	Software usually used on smartphones
Application Systems	A program or set of programs that support a business process. Examples include Tensor and Cygnum.
Bluetooth	A radio standard for short distance communication between electronic devices without using wires. It can be used to connect, for example, computers, mobile phones, earpieces, etc.
C: Drive	See Hard Disk (drive)
Device	General term for a piece of IT equipment (see hardware)
Downloading	Electronically extracting and saving files from a network or the internet to the computer you are using
Encryption	The process of converting data into a coded form to prevent it from being read and understood by an unauthorized party
Hard disk (drive)	Computer storage device, generally fitted inside a PC or laptop – often referred to as the C: Drive
Hardware	Physical components of a computer system, e.g. printer, monitor etc. Often referred to as devices.
ITCSO	The Information Technology Cyber Security Officer (ITCSO) is responsible, in liaison with 3rd party IT Service providers, for applying technical security measures across Estyn's Infrastructure, ensuring compliance with security policies; providing technical assessment of new IT services and applications; providing technical advice and assistance to the Information Governance Group (IGG) and system owners.
IT support	This is your first port of call for all issues and enquiries surrounding IT use within Estyn (itsupport@estyn.gov.wales).
Network	For the purposes of this document the 'Estyn network' is defined as any device connected to Estyn servers or processors by whatever means, encrypted or not

One Drive	This is the area for you to store your personal documents including a backup of your laptop's desktop and document area.
Phishing	This is an attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication
Ransomware	This is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
Removable Media	Refers to data storage devices that can be inserted into a computer to access/store files – e.g. USB memory stick.
Software	A set of computer programmes and instructions that perform a task
Spam	The practice of bulk emailing unsolicited messages.
Trojans	Trojans are virus programs that are hidden within legitimate looking files. They are activated inadvertently – for example by opening an infected email attachment or downloading and running a file from the internet.
USB Devices	USB (Universal Serial Bus) is a standard "plug-in" interface between a computer and add-on devices (such as cameras, scanners, keyboards, printers, etc.). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.
Virus	A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user.
Worms	Worms are virus-like programs that replicate themselves from system to system over a computer network. They often require no human interaction to be able to replicate them.

Appendix A: Frequently asked questions

Personal use of Estyn IT systems

Q1. Can I store my personal photos or media files on my work computer or the network?

A1. We advise you not to store any personal files on an Estyn computer or network – such file may become visible to others, for example, when your computer is being maintained or updated. This storage space is for official records and work-related information only. Work-related documentation which are sensitive, such as your CPM records, are technically accessible by our IT team, but they will never access these documents unless there's a reason for doing so and they have been granted explicit permission. We reserve the right to remove any personal files without notice, for example, a laptop might need to be wiped for security or maintenance reasons.

Q2. Can I use my work equipment for personal online shopping?

A2. Yes, but this is not recommended as it might leave personal data on the equipment. If you do any personal work, it should be during non-working time, off the VPN as otherwise this will be recorded in our network activity log.

Q3. Can I connect my personal OneDrive to my Estyn equipment?

A3. No. You should not connect your personal One Drive to your Estyn Laptop as this may cause syncing issues with our servers. Also, there is a risk that data held in your personal one drive would be visible to our IT support team and/or data held on Estyn equipment may need to be removed for security or maintenance purposes.

Q4. A member of staff is off sick; how do I get access to their email and One Drive?

A4. You should send a request via your line manager to the IT Service Desk, stating the business need for accessing another member of staff's personal account. However, access isn't automatically granted, and your request might be refused. The My site folder on a user's One Drive should already be shared with the line manager.

Q5. A member of staff is off sick; how do I reset their out of office message?

A5. You should send a request via the IT Service Desk, saying why it needs to be changed and what text it should contain.

Q6. Can I use my Estyn email account for personal use?

A6. No

Q7. The rules say that excessive personal use of Estyn email or internet activity during work time systems is considered misconduct. What is classed as 'excessive' personal use?

A7. We define excessive personal email or internet activity as use 'at the expense of Estyn'. This means your personal email or internet use conflicts with the business needs of the organisation. Although the rules suggest a definition of 'reasonable' personal use of email (no more than a handful of messages a week), it is up to individual line managers to decide whether their employees are using email or the internet in a way that adversely affects their performance. This principle also applies to other technology that might be used, such as Teams.

Remote working

Q1. I am working away from the office; can I automatically forward my work emails to a personal email account?

A1. No; this could result in confidential information being forwarded out of the organisation.

Q2. Can I work at home on my own PC?

A2. No – unless this has been approved by your Line manager in discussion with the IT team.

Q3. Can I access my work email or other Estyn internal network applications from a public place, for example a cafe?

A3. Yes - but be aware of the added risks. Public places like cafés are places where eavesdropping can happen easily, and laptop screens can be seen by other customers. Also, these WiFi networks may not be as data secure as our own.

Usernames and passwords

Q1. I am about to go away on holiday. Can I give my password to a colleague so that they can check for important emails while I'm away?

A1. No – you must not give your password to anyone else (you would not lend someone your driving license to drive your car, or your passport to go on holiday). You should turn

on your out-of-office message, and you can give your colleague access to your inbox **through their account** by contacting the IT Service Desk.

Q2. If another person logs on to my computer and stores personal files on it, will I be blamed if they are found on my machine?

A2. No. The username of the person who saved the file is stored in the file data. However, this is another reason you must never share your username or password with anyone else, because you are accountable for any activity associated with your username.

Network security

Q1. Why are so many administrative functions locked down on my desktop?

A1. This is because many administrative functions have the potential to introduce security risks to our network. This is normal practice in an organisation like ours.

Q2. Why is my access to some internet sites blocked?

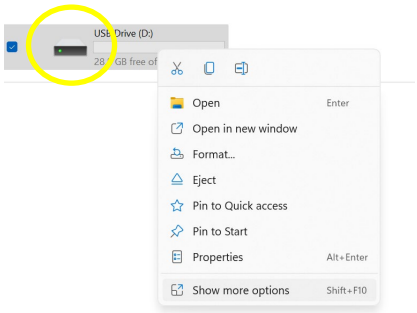
A2. This is to protect staff from inadvertently accessing offensive sites. Some sites can be unblocked on request, but these requests are dealt with on a case-by-case basis depending on the business need. If you would like to make a request to unblock a site, please contact the IT Service Desk.

Q3. Why can’t I download software from the internet?

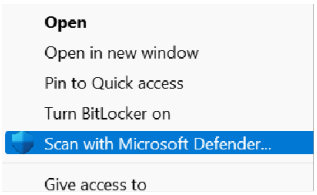
A3. Downloading software leaves our network open to malware and could have possible copyright or licensing implications. This software will also take up capacity on our servers, which is needed to store official information. Installing new software can impact on other programmes or apps, so software must be approved, and impact tested before it can be installed. If you need the software for business purposes, you should contact the IT Service Desk.

Q4. How do I virus check removable media?

A4. Individual files are automatically checked when they are accessed and opened. However, it is good practice to check the complete device using Microsoft Defender on your laptop. This can be run at any time by right clicking on the device and choosing to show more options:



Then choose Scan with Microsoft Defender:



Q5. Someone I know has emailed me a warning about a virus. What should I do?

A5. Forward the email to itsupport@estyn.gov.wales

Q6. I want to download an app to my Estyn smartphone. What should I do?

A6. You should send a request to itsupport@estyn.gov.wales

saying what the app will be used for and whether there are any costs.

Protecting information

Q1. I have received a document that has a protective marking from another organisation. How should I treat it?

A1. You should apply the appropriate protective marking for the document's content. Most commercially sensitive material would need a 'OFFICIAL – maintain commercial confidence when sharing'. For more information on government protective markings, see our Information Assurance Policy.

Q2. Can I use my C: Drive to store information?

A2. Yes, but you should note that only specific folders 'Documents' and 'Pictures' on your C: drive are backed up. It is recommended that you use your One Drive to ensure information is backed up.

Appendix B: Email and internet – Do's and Don'ts

Do:

- Ask for confirmation of email receipt/read when you feel this is important
- Check your email daily when working
- Turn on your 'Out of Office' message when you're absent from work
- Reply promptly (not necessarily immediately) to all email messages that need a reply. If this isn't possible, send an acknowledgement of receipt explaining when you'll be able to send a more comprehensive response
- Refer any suspect emails or files to the IT team for checking

Don't:

- Attempt to circumvent security systems or procedures
- Apply incorrect protective security markings to data
- Access pornography or other inappropriate material via the internet at any time
- Share personal passwords so that others can log on as you
- Use anyone else's password or allow others to use yours
- Transmit copyrighted material without permission
- Send emails to the press
- Subscribe to any personal mailing lists, newsgroups or any other internet-related service using your work email
- Open suspicious email attachments or executable files without first seeking advice from the IT Team. This includes clicking links in suspicious emails (Phishing).
- Send emails containing pornography or potentially criminal material
- 'Spam' internet users via the Estyn internet system, using your Estyn email address
- Impersonate any other person when using the email or amend messages received
- Send emails to large user groups unless it's necessary. Consider whether there is not a more appropriate form of communication, (e.g. Your Update, Works Matter, etc.)
- Add new recipients into email threads without considering whether it is appropriate for them to see the whole content or better to begin a new thread
- Make excessive personal use of the internet, such as instant messaging, during work time

Please refer to Appendix C for more guidance on using email.

Appendix C: Guidelines on the effective use of email

These guidelines will help you establish efficient practices for handling email and avoid many potential pitfalls.

Managing your email

Email is an essential means of communication. However, if you don't manage your emails effectively, it can be a drain on your productivity and become stressful.

Opening your emails as new messages arrive can be very disruptive to your working day. If an incoming email message distracts you from productive work, it takes an average of four minutes to get back on track. So, in one day, if 15 emails derail you, you've lost an hour of productive time. By establishing efficient practices for dealing with email, you can take control of your working day:

1 Wherever possible talk instead of type! It’s easy to overuse emails to communicate. It’s often quicker to pick up the phone.

2 Managers should be careful not to encourage unhealthy expectations – staff shouldn’t feel that they must respond to emails immediately, out of hours, when on leave, etc., unless it’s part of their role.

3 Clear out your inbox – it reduces clutter and stress. Don't store emails in your inbox, move them into folders. A cluttered inbox risks items being overlooked, missed or forgotten. It’s also stressful to open your inbox at the beginning of the day to hundreds of messages. By keeping a clear inbox, you can take charge of your day and your work priorities.

4 Avoid any folder becoming too large. Large folders are difficult to manage and are slow to open. Delete old or irrelevant messages regularly to improve loading times.

5 Manage when you check your email. Make sure you check it as often as required to carry out your role but try to set specific time aside to deal with emails. It can help to block out time when you can work on other operational or strategic work without interrupting your productive flow. For example, you might choose to check your email five or six times a day. Consider switching off any desktop pop-ups or sound alerts when new messages arrive, so that you have more control over your working day.

6 Try to avoid using email for urgent matters. If you regularly flag messages as urgent, it creates an environment where people feel they must view each email as they get it. Use the "three hour" rule – for anything that requires a response within three hours

use other alternative communication methods such as telephone or Teams message or face-to-face when this is an option.

New messages

Replying

1 Think before you hit "reply-all". Ask yourself whether everyone on the recipient list really needs to see your reply. This can be a major inconvenience for some of the recipients.

2 Stop and think before you hit the Send button. If you are angry or upset about the message you're replying to, give yourself some time to calm down before replying. Sending a quick and angry response doesn't help and often leads to more awkward messages being sent.

3 Paste responses to common queries. Keep a list of responses to frequently asked questions to save time when you reply. Alternatively, consider uploading the information on SharePoint and then send your recipient the link (URL).

4 Take care when replying to email lists; be very careful to direct your reply to the appropriate address. Often a person should reply to an individual but instead sends that reply to the entire list.

Forwarding

1 When you forward messages, consider including a summary at the beginning. This will help the new recipient to catch up on what has already been discussed. You can also include the actions or information specific to that person so that they can quickly provide the response you need.

2 Remember your legal obligations - never send or forward messages containing libellous, defamatory, offensive, discriminatory or obscene remarks.

3 Never forward virus hoaxes and chain letters. If you receive an email warning you of a virus that will damage your PC, it is almost certainly a hoax. Sometimes virus hoaxes contain viruses themselves! Email chain letters usually promise rewards or ask for your support for a charitable cause. Even if the message seems legitimate, the name of the sender could be faked. If a message seems to be too good to be true, **it probably is**, so just delete these messages.

Attachments

1 Be very careful when opening attachments, even if the message appears to be from someone you know. Attachments containing viruses are one of the most widely used methods for infecting PCs.

2 Be selective about sending of attachments. If you can, either include the text in the body of the email or, even better, save the file in SharePoint and then send a link it.

3 Consider the file format of the attachment. Make sure in advance that the recipient has the right software to view the attachment. For example, someone outside Estyn might not have the latest version of Word installed.

4 Be careful about the size of an attachment. Files in text (txt), revisable text format (rtf) and portable document format (pdf) are usually more compact formats than files in Word (docx) format. Images in documents can result in very large file sizes.

Legal issues

1 Email policy and regulations, including misuse of email, are explained earlier in this policy.

2 **Data Protection** – The General Data Protection Regulations 2016 applies to computerised records, and this includes email. It's important that staff don't keep email messages containing any personal information for longer than that information is required. The length of time an email with personal data should be retained depends on the purposes for which the information was obtained. Once this purpose is complete, the email should be deleted. For further information please see the Information Assurance policy on our website.