Isle of Anglesey County Council
IT Acceptable Usage Policy

Version 2.1.2 (updated December 2025)

About this policy

The council provides many essential services and business functions which rely on IT technology resources. The use of IT resources must be in line with good professional working practices, procedures and must ensure the security and integrity of all council information and data.

The purpose of this policy is to establish how the council's IT facilities and resources must be used. The scope of this policy extends to all services, employees, elected members, contractors, vendors and partner agencies who use/access the council's IT facilities.

Note: This document contains content generated by Artificial Intelligence (AI). AI generated content has been reviewed by the author for accuracy and edited/revised where necessary. The author takes responsibility for this content.

Revision history

Version	Date	Summary of changes
1.1	6 April 2018	Amended following comments from the IT Governance Board
1.2	26 April 2018	Amended following further comments from Y Penaethiad
1.3	16 July 2019	Amended to clarify guidance on Bring Your Own Device
1.4	2 February 2022	Updated following audit review
2.0	21 May 2025	Amended following review, and updated to incorporate aspects previously held in a seperate policy
2.1	30 June 2025	Amended following consultation with Leadership Team
2.1.1	24 September 2025	Amended following further consultation with Leadership Team
2.1.2	9 December 2025	Amended following further consultation with Leadership Team and change of service

Date of next review

This policy will be amended regularly in response to changing circumstances as digital technologies develop and in response to operational and legislative requirements.

This document will be reviewed in December 2026.

This document will be reviewed by the Chief Digital Officer.

Contact details

Mathew Henshaw

Chief Digital Officer

MathewHenshaw@ynysmon.llyw.cymru

We are happy to provide this policy in alternative formats on request. Please use the above contact details.

Mae'r ddogfen yma ar gael yn y Gymraeg This document is available in Welsh

Contents

1. Introduction 4
2. Purpose 4
3. Scope 4
4. Policy statement 4
   - 4.1 Computer use 4
   - 4.2 Internet usage 5
   - 4.3 Email usage 6
   - 4.4 Instant messaging 7
   - 4.5 Social media usage 8
   - 4.6 Security 8
   - 4.7 Antivirus 8
   - 4.8 Monitoring 8
   - 4.9 Personal devices 9
5. Breaches of policy 9
6. Weblinks 9

1.Introduction

1.1 The council provides many essential services and business functions which rely on Information Technology (IT) resources. The use of IT resources must be in line with good professional working practices, procedures and must ensure the security and integrity of all council information and data.

2.Purpose

2.1 The purpose of this policy is to establish how the council's IT facilities and resources must be used.

3.Scope

3.1 The scope of this policy extends to all services, employees, elected members, contractors, vendors and partner agencies who use/access the council's IT facilities.

4.Policy statement

4.1 Computer use

4.1.1 All users of council IT must ensure at all times that:

- authorisation has been provided to use the IT facilities with a domain username and password provided by the Digital, Data and Technology (DDaT) Division
- user and system account logon passwords are kept confidential and are not shared, displayed or communicated to anyone who does not have a legitimate right to that information
- council information and data are stored logically and in accordance with information governance arrangements and in locations that are sufficiently resilient to network and system outages

> Please note, mobile computing devices such as digital cameras and digital dictation devices, must not be treated as data storage devices – however, the council accepts that photographs/audio files for council purposes can also be classed as data and recommends that any photographs/audio files taken are removed from the device(s) and stored on the council network as soon as possible. Unless for work purposes, if fitted with a geotagging (location identification) feature, this should be switched off.

- screens/computers are locked by users when away from the computer

- unauthorised, nonstandard equipment is not connected to a computer in any way
- software is not installed on council IT computer equipment by unauthorised staff– the DDaT Division staff will only install software and hardware procured in partnership with the DDaT team where the due diligence and assurance process haven't indicated any unacceptable risks.
- council's IT equipment must not be used to store any personal data such as wedding photos, music files, and so forth
- computers and network components are not mishandled, wilfully damaged or tampered with in any way – this includes unauthorised third party repair, or removing of any screws or fixings
- any suspicious or unknown equipment near or around PCs/laptops is reported to the IT Service Desk
- computers are logged off and shut down when not in use for extended periods (including overnight) and monitors are powered off
- personal cloud based IT facilities such as Dropbox are not used to store work related information - work related documents which are intended for shared use can be saved to the OneDrive drive on your workstation
- work related data is not emailed to personal email accounts for access from non council devices

4.2 Internet usage

4.2.1 The following principles will apply when using the internet on council owned devices:

- reasonable personal use of the internet is allowed if permitted by your line manager - the line manager is responsible for ensuring that usage is reasonable
- you must not use the council's internet or email systems for trading or personal business purposes
- the council has in place a process to block categories of internet sites and individual sites if it is deemed appropriate
- if you use the internet to buy goods or services, the council will not accept liability for default of payment or for security of any personal information you provide
- downloading of video, music files, games, software files and other computer programs for nonwork related purposes is strictly prohibited - these types of files consume large quantities of storage space on the system and may violate copyright laws
- for the use of Artificial Intelligence (AI) please refer to the Generative AI Policy

4.2.2 Many internet sites that contain unacceptable content are blocked automatically by the council's systems. However, it is not possible to block all 'unacceptable' sites electronically. You must not therefore deliberately view, copy or circulate any material that:

- is sexually explicit or obscene

- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains images, cartoons or jokes that will cause offence

4.2.3 If your role requires you to access such material for legitimate work purposes (for example, safeguarding, research, or case management), ensure you follow the formal exception process and seek appropriate advice before proceeding.

4.2.4 Any such exceptions should:

- be strictly limited to scenarios where access is directly relevant to professional duties and necessary for fulfilling job responsibilities
- be authorised in advance by a line manager, DPO, or other appropriate authority
- be documented, with the purpose and scope of access clearly recorded
- comply with all relevant data protection and safeguarding regulations

4.2.5 The council records the details of all internet traffic. This is to protect the council and its employees from security breaches, including hacking and to ensure that 'unacceptable' sites are not being visited.

4.3 Email usage

4.3.1 Personal use of llyw.cymru and gov.wales email is not permitted at any time.

4.3.2 It is inappropriate to use your council email address for personal use as it may give the impression that any business is on behalf of the council.

4.3.3 You must not use the email system in any way that is insulting or offensive.

4.3.4 You must not deliberately view, copy or circulate any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains unwelcomed propositions
- involves gambling, multiplayer games or soliciting for personal gain or profit
- contains images, cartoons or jokes that will cause offence
- brings the council into disrepute or exposes it to legal action

4.3.5 If your role requires you to access such material for legitimate work purposes (for example, safeguarding, research, or case management),

ensure you follow the formal exception process and seek appropriate advice before proceeding.

4.3.6 Any such exceptions should:

- be strictly limited to scenarios where access is directly relevant to professional duties and necessary for fulfilling job responsibilities
- be authorised in advance by a line manager, DPO, or other appropriate authority
- be documented, with the purpose and scope of access clearly recorded
- comply with all relevant data protection and safeguarding regulations

4.3.7 The council routinely produces monitoring information which summarises email use and may lead to further investigation being undertaken.

4.4 Instant messaging

4.4.1 Use of instant messaging services for work purposes is limited only to corporately approved services, directly linked to staff login credentials, such as Microsoft Teams.

4.4.2 Use of other external messaging services, such as What's App, is prohibited as a means of council communication unless a business case has been developed and approved by the Data Protection Officer (DPO) and DDaT Section.

4.4.3 Messaging services must not be used in any way that is insulting or offensive.

4.4.4 You must not deliberately view, copy or circulate any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains unwelcomed propositions
- involves gambling, multiplayer games or soliciting for personal gain or profit
- contains images, cartoons or jokes that will cause offence
- brings the council into disrepute or exposes it to legal action

4.4.5 If your role requires you to access such material for legitimate work purposes (for example, safeguarding, research, or case management), ensure you follow the formal exception process and seek appropriate advice before proceeding.

4.4.6 Any such exceptions should:

- be strictly limited to scenarios where access is directly relevant to professional duties and necessary for fulfilling job responsibilities
- be authorised in advance by a line manager, DPO, or other appropriate authority
- be documented, with the purpose and scope of access clearly recorded
- comply with all relevant data protection and safeguarding regulations

4.5 Social media usage

4.5.1 Please refer to the council's Social Media Policy[i].

4.6 Security

4.6.1 The council's computer systems are under continuous cyber threat. The council must apply mitigations and technological solutions in order to safeguard information and data and to protect the security and integrity of all IT systems.

4.6.2 Users of all council computers and devices must ensure that:

- computers/devices are not given to any unauthorised persons for safe keeping
- computers/devices are not left discarded or unattended in public places
- all portable mobile computing devices and other IT equipment should not be left unattended in any vehicle at any time
- computers/devices must be adequately protected from physical damage
- computers/devices are not hired, lent or given out without authorisation from the Digital, Performance and Modernisation Service
- all computers/devices which are no longer required, or which have reached the end of useful life must be returned via the line manager to the DDaT Service Division, to be disposed of through the council's IT disposal procedure

4.6.3 Use of council computers and devices outside the UK is not permitted, unless exceptional circumstances are identified as per the IT Security Policy[ii].

4.6.4 Devices retained as pool or spare devices by services will not remain compliant with council policies and will be remotely wiped.

4.7 Antivirus

4.7.1 Any warnings visible on screen from the council's antivirus/antimalware software about identified/detected threats from viruses/malware should be reported to the IT Service Desk immediately.

4.8 Monitoring

4.8.1 Routine monitoring is applied to all users of the internet and email system supplied by the council. Short term monitoring may also be undertaken on an individual or group of individuals in response to a particular problem or need.

4.9 Personal devices

4.9.1 Personal devices which are not the property of the council, including mobile phones, Personal Digital Assistants (PDAs), digital pens, and so forth, must not be used to locally record or capture information relating to the council and its services including audio recordings, photographs and video recordings.

4.9.2 Where a personal device is to be used it should only be through supported methods in accordance with the Bring Your Own Device (BYOD) scheme as outlined in the IT Security Policy. Using these methods ensures data is only stored within a secure and managed environment.

4.9.3 Personal devices must not be used to record meetings, conversations or events under any circumstances. Any covert recordings, whether on personal or council owned devices, are in breach of data protection requirements and may be treated as misconduct within the council's disciplinary procedures.

5.Breaches of policy

5.1.1 Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to council assets, or an event which is in breach of the council's security procedures and policies.

5.1.2 All council employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the council's Incident Reporting Procedure, as set out in the IT Security Policy. This obligation also extends to any external organisation contracted to support or access the information systems of the council.

5.1.3 The council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

6.Weblinks

[i] https://monitor.anglesey.gov.wales/policies/human-resources/Social-Media-Policy.pdf
[ii] https://monitor.anglesey.gov.wales/policies/information-technology/IT-Security-Policy.pdf