RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

ELECTED MEMBER ICT, INTERNET & EMAIL ACCEPTABLE USE POLICY

Version 4

Document Information

Version:	4
Status:	Final Approved
Date:	13th July 2026
Owner:	Tim Jones, Service Director – ICT & Digital Services
Author:	Louise Evans, Data Protection & Improvement Officer

CONTENTS

1. INTRODUCTION

The Council considers the use of ICT equipment, internet and email to be a valuable asset that if used correctly can help Elected Members undertake their job more effectively. Therefore, it is Council policy to promote its proper and efficient use.

This policy defines what the Council considers as acceptable use of its ICT equipment, internet and email facilities and sets out rules and guidelines for its access and use.

The overall purpose of these conditions is to:

- promote efficient and safe use of Council managed ICT equipment, devices and systems, including the Councils internet and email facilities;
- protect the Council and its Members from legal action, either civil or criminal;
- protect and safeguard information, and
- ensure compliance with relevant legislation.

2. SCOPE

Acting in Official Capacity as Part of the Council

This policy applies whenever Members are acting in their official capacity as part of the Council, such as participating in committees or undertaking formal Council business.

When acting in this capacity, Members must only use Council managed equipment, devices, and systems. This includes internet and email facilities provided by the Council.

The policy applies at all times, regardless of whether access is local or remote (e.g., from a Council office or a Member's home) and regardless of the type of device used. This includes all Council managed devices such as iPads, desktop computers, laptops, and mobile phones.

Representing Residents

Members should note that when representing residents, they act as data controllers for any personal data processed and are registered with the Information Commissioner's Office in this regard.

Members should use Council managed equipment, devices and systems when representing residents. The use of Council systems is strongly encouraged, particularly where the casework relates to Council services, as this enables information to be handled securely within the Council's ICT environment and allows appropriate support, monitoring and security controls to be applied.

When using Council managed equipment, devices and systems for constituency work, Members must comply fully with this policy.

Where appropriate, Members should inform constituents that Council email systems are being used and that any email exchanges may be subject to Council monitoring, as outlined in Section 14.

Political Party Use

Members are not permitted to use Council managed equipment, devices, or systems for any activities associated with representing a political party, including during election periods.

Exclusions

The policy does not include guidance on the acceptable use of social media such as blogs, message board, social networking (e.g. Facebook, Twitter, LinkedIn) and content sharing websites (e.g. Flickr, Youtube). This is covered separately under the Council's Social Media Policy. The full document is available on the Members Portal.

3. RELATED POLICIES

Members should refer to the full list of related policies and procedures outlined in Appendix III. These documents provide essential guidance on key areas including information security, email use, Welsh language responsibilities, and professional conduct. All documents are available on the Members Portal.

4. ACCESS TO COUNCIL SYSTEMS AND APPLICATIONS

Access to Council emails, Committee papers via Modern.Gov, Teams, Zoom, the Members Portal, and other related applications is only available through authorised Council managed devices.

If a Member wishes to access Council systems and data from outside the UK, they must contact the Head of Democratic Services (or a delegated officer) in advance to discuss their requirements. Subject to approval, the Head of Democratic Services will work with ICT and Digital Services to make appropriate arrangements to ensure secure access can be provided. To protect Council systems and data, the Council reserves the right to restrict or block access to Council systems depending on the location being visited, the level of risk identified, or where secure access cannot be assured.

5. INTERNET CONNECTIVITY

Members should seek to establish a reliable and effective internet connection when attending Council Committee meetings through the hybrid facilities and attend meetings in accordance with the requirements of the Council's Multi Location Meeting Policy.

6. SECURITY UPDATES & MAINTENANCE OF COUNCIL MANAGED ICT EQUIPMENT, DEVICES & SYSTEMS

Members shall ensure that all Council managed ICT equipment, devices and systems remain up to date and compliant with security requirements. Security updates and other essential maintenance issued by ICT must be permitted to install without delay. Members shall not disable, defer, or otherwise interfere with these updates.

7. OWNERSHIP AND RETURN OF COUNCIL ICT EQUIPMENT

All ICT equipment provided by the Council shall remain the property of the Council and must be surrendered to the Council in the event that a Member ceases to be an Elected Member. In this event access to any Council electronic device will be suspended and terminated within ten working days.
Council managed devices must also be returned promptly when requested as part of routine ICT support and cyber security operations.

8. REPORTING LOST OR STOLEN ICT MANAGED EQUIPMENT & DEVICES

If a Council managed device is lost or stolen, Members must report the incident immediately upon discovery to the Head of Democratic Services (or delegated officer), who will notify the Council's ICT Service Desk. This is so that immediate action can be taken to secure any Council data stored on the device and reduce the risk of unauthorised access.

Further information on how to report such incidents and the steps involved, please refer to the Council's 'Procedure for **Reporting** Information Security Incidents and Events'. This should be read alongside the 'Procedure for **Investigating** Information Security Incidents and Events', both of which are available on the Members Portal.

9. REASONABLE PERSONAL USE

Members may use Council ICT equipment, internet, and email facilities for reasonable personal use, provided that such use:

- is used in a members own personal time
- does not interfere with the performance of official Council duties
- does not take a priority over Council work responsibilities
- does not incur expense on the Council
- does not have a negative impact on the Council in any way, nor damage its reputation
- complies with the guidance set out in this and wider council policies

Subject to this policy, personal use could include but is not solely restricted to areas such as online banking, shopping, entertainment, leisure activities or bookings, personal research.

Members may use their Council email account (@rctcbc.gov.uk) for reasonable personal communications. However, it must not be used to sign up for non-work-related subscriptions, mailing lists, online services, or used to register with external organisations, as this may increase cyber security risks and expose Council systems to unwanted or malicious communications.

Members should note that such personal use is a privilege and not a right, which can be removed at any time.

Any personal use is carried out at the Member's own risk and the Council does not accept responsibility or liability for loss caused as a result of use.

Members should note that use of Council ICT systems may be subject to monitoring in accordance with Section 15 of this policy.

10. ICT POINTS OF CONTACT

The ICT Service Desk is the first point of contact for all enquires, queries and support problems relating to Council managed ICT equipment, internet and email facilities and/or any other ICT issues.

ICT Service Desk Hours:

- Monday – Friday 08:00-17:00

Contact Details:

- **Telephone:** 01443 570000
- **Email:** ictservicedesk@rctcbc.gov.uk

Alternatively, Members Services can help Members and log a request on their behalf.

11. TRAINING

Members must undertake appropriate ICT, Cyber Security and Data Protection training as part of their induction programme. Members should always take forward any mandatory training as promoted by the Head of Democratic Services and the Service Director, Digital and ICT during their term of office.

Additional individual training needs should be discussed with the Head of Democratic Services or through the Member Personal Development Review.

12. WELSH LANGUAGE ACT

Welsh is an official language in Wales, and members of the public have the right to communicate with the Council and its Members in Welsh. This includes all forms of correspondence, such as emails sent and received.

To understand your responsibilities under the Welsh Language Act, please refer to the Council's Welsh Language Scheme and Welsh Language Standards (RCT). Both documents are available on the Members Portal.

13. INTERNET & EMAIL GENERAL RESTRICTIONS OF USE

General restrictions applicable to the use of the Council's internet and email facilities are set out in Appendix I.

14. EMAIL GOOD PRACTICE

Elected Member email 'good practice' are set out in Appendix II.

15. MONITORING, AUDIT & ENFORCEMENT

The use of Council managed ICT equipment, devices and systems including the Council's internet and email is a valuable business tool, however, misuse of these facilities can have a negative impact on the Council and Members. Appropriate monitoring, audit and enforcement is therefore required to support proper and efficient use.

There is no routine surveillance of Elected Members' use of Council ICT systems. The Council does, however, operate proportionate and necessary monitoring across its systems for security, audit and business purposes. This includes automated monitoring to help protect Council systems, data and users, for example by identifying spam, phishing emails and other cyber security risks. This type of monitoring is preventative in nature and is not undertaken to view the content of individual communications.

- Council systems and any data held on them in relation to Council business, including emails, documents and other information, are the property of the Council.

- The Council reserves the right to access, monitor and review any Member's use of Council managed ICT equipment, systems, facilities and data covered by this policy (and related Information Management & Information Security policies), without additional consent being required from the Member. The Council also reserves the right to bypass any security setting applied by a Member (e.g. password), subject to the authorisation of the Council's Monitoring Officer and Service Director – Digital & ICT.

- Whilst all activity is recorded (e.g. internet browser history, @rctcbc.gov.uk email traffic etc), any access to, and review of such equipment, activity and data will be undertaken strictly to the extent permitted or required by law, and only where necessary and proportionate for legitimate Council business purposes, including audit and security, or where there is reason to believe that a breach of security, breach of policy or misconduct has occurred (see section 10). Where more detailed access is required, including access to the content of communications, this will be undertaken on a case-by-case basis, subject to appropriate authorisation, formally logged for audit purposes, and limited to what is necessary for the specific purpose.

- The Council reserves the right to make and retain copies of all information, including, but not limited to, emails and data documenting the use of the internet and email systems, for the purposes set out above. Members should be mindful of this when using Council managed ICT equipment and/or systems for personal use.

- The Council reserves the right to place restrictions on the use of internet and email accounts at any time.

16. BREACH OF POLICY/ENFORCEMENT

Any Member who considers that this policy and/or any other Information Security policy has not/is not being followed are encouraged to raise the matter with the Council's Monitoring Officer (or his delegated officer) in the first instance.

Subject to the recommendation of the Councils Monitoring Officer, where there is a suspected breach, this will be reported to the ICT Service Desk on the Member's behalf, and an investigation will be undertaken in line with the Council's 'Procedure for

Investigating Information Security Incidents and Events', which is available on the Members Portal.

In certain circumstances an investigation may lead to a Member's ICT access privileges being revoked and possible action being taken against a Member in accordance with the Council's Members Code of Conduct.

APPENDIX I

ELECTED MEMBER ICT EQUIPMENT, INTERNET & EMAIL – GENERAL RESTRICTIONS OF USE

Council managed ICT equipment, devices and systems including the Councils internet and email facilities **must not** be used for:

- Any Party political reasons or political lobbying i.e. the process of making a concerted effort designed to achieve a political result that is against Council policy or goals. This could then in turn be harmful or cause issue for the Council.

- Engaging in any illegal activity or accessing / storing material that is profane or obscene (pornography), that incites illegal acts, violence or discrimination towards other people (hate literature).

- Accessing/using online gambling web sites, blogs or chat rooms that are offensive, unsuitable or inappropriate to the workplace

- Engaging in inappropriate language, designated as: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful. This applies to any public or private messages, images, audio and to any material posted on web pages. Engaging in personal attacks, including prejudicial or discriminatory to other people.

- Posting information/material that could cause damage or a danger of disruption to Council business.

- Attempting to gain unauthorised access to the internet or go beyond their authorised access. This includes attempting to log in through another person's account or accessing another person's files. Sending emails purporting to come from some other person, whether or not that person is an employee or Elected Member of the Council. Making deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.

- Harassing another person. Harassment occurs when a person engages in unwanted conduct which has the purpose or effect of violating a person's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that person. If users are told by another person to stop sending them messages, they must stop. Further guidance on harassment is available through the Council's Antibullying & Harassment Policy.

- Knowingly or recklessly posting false or defamatory information about a person or organisation.

- Posting, forwarding or replying to email chains or correspondence or engaging in "spamming". (spamming is the word used to describe the sending of marketing, annoying or unnecessary messages to a large number of people).

Members who may be required to undertake any of the prohibited actions set out above (in relation to their official Council duties) and/or require legitimate business access to internet sites that are 'blocked' by the Councils web filtering policy should discuss their requirements with the Council's Monitoring Officer.

APPENDIX II

ELECTED MEMBER EMAIL GOOD PRACTICE (@rctcbc.gov.uk)

1. EMAIL ACCESS

All Members are allocated a Council email account to conduct Council and Constituency business (representing residents). The email account is in the format of: <name>@rctcbc.gov.uk.

Elected Members are **not permitted** to use any other email account e.g. a personal gmail / hotmail account etc., for these purposes.

2. EMAIL ACCOUNT SECURITY

ICT & Digital Services will provide Members with a user account and password; this also controls access to a Members email account.

Members are responsible for their individual access and email account security and must take all reasonable precautions to prevent their account from being compromised. This includes sharing and divulging of account details.

3. ACCESS BY OTHERS

Members must not allow any other person to access Council systems or applications using their account credentials. This includes, but is not limited to, email accounts, the Members' Portal, Modern.Gov, Teams, and any other Council-provided ICT services and systems.

Access must only be granted for legitimate Council business purposes and under no circumstances should Members share their login credentials or passwords. Where access by another **authorised** person is required (for example, a colleague needing temporary access to a mailbox during the Member's absence), this must be arranged through the appropriate account security permissions to ensure a clear audit trail and maintain system security.

Members should contact the ICT Service Desk for advice and guidance on how to set up delegated access correctly.

4. STAYING SAFE WHEN USING EMAIL

Malware, short for malicious software, is software or computer code that is designed to damage files or entire computer systems, steal data, or disrupt networks. Some of the most common type of malware include viruses, ransomware, spyware, worms and spam. One of the most common routes for malware to penetrate a computer or network is through email. RansomWare is another form of malicious software that renders information inaccessible with a Ransom attached for payment. These are everyday risks for the Council.

Whilst ICT blocks the vast majority of unwanted or spam email through its automated monitoring systems, with scams becoming more and more sophisticated it may be possible for some malicious emails to reach a Member's mailbox.

It is therefore important that Members are aware of the dangers, know what to look out for and know how to protect themselves when using email.

	Members are required to familiarise themselves with the Council's guidance **'Staying Safe when Using Email'** guidance, which provides practical advice and information on key warning signs of scams. This document is available on the Members Portal.

If a Member suspects that malware may have infected their device or the Council's network, they must take immediate action to contain the situation and prevent the malware from spreading to other devices and parts of the Council's network.

The following **immediate action** must be taken:

Step 1:	**DO NOT open the attachment or click on the hyperlink.**
Step 2:	**If using a mobile device, disconnect it from the WIFI.** **If using a PC, remove the network cable from the drop point.**
Step 3:	**Turn off the power on the device.**
Step 4:	**Report the call by telephone (01443 425080) to the ICT Service Desk providing as much information as possible in particular, in relation to the last actions undertaken on the device/PC (links clicked, websites visited etc).**
Step 5:	**Follow the instructions given to you by the ICT Service Desk.**
Step 6:	**Report the matter to the Head of Democratic Services or a Member of the Council Business Unit.**

5. EMAIL MESSAGE SECURITY

Internal emails i.e. those sent to and from council emails accounts ('@rctcbc.gov.uk') accounts are transmitted within the Council's network and are therefore deemed to be secure.

External emails, sent outside the Council's network are transmitted across the open internet and could potentially be liable to interception, changing or loss. Extra caution should be taken when transmitting personal, sensitive and/or confidential information externally in this way.

Members must ensure that email is the most appropriate method of transfer that should be used. If email is deemed the most appropriate, Members must adhere to the good practice contained within the following guide, to reduce the potential risks associated with emailing personal information i.e. the email being sent to the wrong recipient or wrong attachment being sent etc.

Further support and guidance on this is contained within the Council's guidance **'Transferring of Personal Information'** guidance, which is available on the Members Portal.

If users are required to email personal or commercially sensitive information to external recipients on a regular basis, the use of the Council's secure email facilities may be appropriate. Members should discuss their requirements with the Head of Democratic Services.

6 EMAIL SIGNATURES

A form of good practice is to take forward bilingual signatures on each email, outlining details relating to Elected Member contact details and the Electoral ward represented. Members may wish to take forward their preferred pronouns within their signature, although this is an individual choice and preference for each Member. Guidance and support in creating an email signature can be provided to Members through contacting the Democratic Services Team.

7. EMAIL DISCLAIMER

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support RCTCBC business should be considered to be an official communication from the Council.

In order to ensure that the Council is protected adequately from misuse of e-mail, all external e-mail must carry the following disclaimer which will be **added automatically** on transmission from the Council:

Croesawn ohebu yn Gymraeg a fydd gohebu yn y Gymraeg ddim yn arwain at oedi. Rhowch wybod inni beth yw'ch dewis iaith e.e. Cymraeg neu'n ddwyieithog.
Mae'r neges ar gyfer y person / pobl enwedig yn unig. Gall gynnwys gwybodaeth bersonol, sensitif neu gyfrinachol. Os nad chi yw'r person a enwyd (neu os nad oes gyda chi'r awdurdod i'w derbyn ar ran y person a enwyd) chewch chi ddim ei chopïo neu'i defnyddio, neu'i datgelu i berson arall. Os ydych chi wedi derbyn y neges ar gam, rhowch wybod i'r sawl sy wedi anfon y neges ar unwaith. Mae'n bosibl y bydd holl negeseuon yn cael eu cofnodi a/neu fonitro unol â'r ddeddfwriaeth berthnasol. I ddarllen yr ymwadiad llawn, ewch i http://www.rctcbc.gov.uk/CY/Help/TermsOfUse.aspx

We welcome correspondence in Welsh and corresponding with us in Welsh will not lead to a delay. Let us know your language choice if Welsh or bilingual.
This transmission is intended for the named addressee(s) only and may contain personal, sensitive or confidential material and should be handled accordingly. Unless you are the named addressee (or authorised to receive it for the addressee) you may not copy or use it, or disclose it to anyone else. If you have received this transmission in error please notify the sender immediately. All traffic may be subject to recording and/or monitoring in accordance with relevant legislation For the full disclaimer please access http://www.rctcbc.gov.uk/disclaimer

8. EMAIL CONTENT DISCLOSURE

Email messages sent and received in relation to official Council business may be disclosed under the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, or in legal proceedings, in the same way as paper documents.

Members should take care with the content of email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Members should assume that email messages may be read by others and not include anything that would offend or embarrass any reader, or themselves, if it found its way into the public domain.

Deletion from an email user's inbox/sent items etc. does not mean that an email cannot be recovered; all email messages should be treated as potentially retrievable.

Members should note that when representing residents, emails may also be disclosable under relevant legislation. As Members are data controllers for the data contained within such communications, any information requests relating to data held in these emails should be made directly to the Member. Such requests will be handled separately by the Member, with support from relevant Council teams where required, such as Members Services and Information Management.

9. GLOBAL/MASS EMAIL COMMUNICATIONS

In order to ensure that the Council's email system is able to preform to its optimum, Members are not permitted to use the Council's email system to send emails to mass recipients (i.e. emails to 75 recipients or more in one instance).

Should a Member need to send a communication to a large number of recipients, whether internal or external, they should first discuss their requirements with Member Services, who will advise on the most appropriate and effective method of communication.

Members should also take care when using the 'reply to all' feature, ensuring that only intended recipients of the email are copied in to the communication response.

10. USE OF BLIND CARBON COPY (BCC)

When sending an email to multiple recipients, the 'BCC' function must be used where there is a requirement to protect the confidentiality of a recipient's email address/identity.

11. HOUSEKEEPING

The Council has set a limit on the size of mailboxes, which includes Inbox, Sent Items and Deleted Items. Members will receive an automated reminder as that limit is approached and unless action is taken to reduce its size, no further emails will be accepted or sent for that person until action is taken.

It is the responsibility of each Member to manage their mailbox. Good practice is to manage email accounts like any other filing system. Members should regularly carry out 'housekeeping' of their mailbox:

- Read and delete emails regularly.
- Keep your 'Inbox', and 'Sent' folder contents to a minimum.
- Regularly delete 'Deleted items' and associated sub-folders.

12. USE OF OUT OF OFFICE ASSISTANT

Members should use the "Out of Office Assistant" if they know they will not be able to access their mailbox for a period of time. Good practice is to explain when you will be returning to work and whom the person can contact in your absence to deal with queries. The Out of Office message must be professional in its content and bilingual.

13. EMAIL ETIQUETTE

When creating, writing and responding to email messages, Members must be polite and use appropriate language as they would with any other form of communication such as, telephone or letter.

Members must ensure that they adhere to the Council's guidance **'Email Practices & Etiquette'**, which is intended to promote consistent and professional email etiquette across the Council. This guidance is available on the Members Portal.

APPENDIX III

RELATED POLICIES & PROCEDURES

The following policies and procedures are available in full on the Members Portal. Members are encouraged to familiarise themselves with these documents to ensure compliance with relevant standards and responsibilities:

1.	Procedure for **reporting** information security incidents and events
2.	Procedure for **investigating** information security incidents and events
3.	Welsh Language Scheme
4.	Welsh Language Standards
5.	Antibullying and Harassment Policy
6.	Guidance: Staying safe when using email
7.	Guidance: Transferring Personal Information
8.	Guidance: Email practices and etiquette
9.	Social Media Policy
10.	Multi Location Meeting Policy
11.	Policy: Acceptable Use of Teams

APPENDIX IV

ELECTED MEMBER POLICY CONSENT FORM

Policy Name	Elected Member Internet & Email Acceptable Use Policy
Version Number	4.0
Date	13th July 2026

Members are not required to re-sign this policy following minor updates. However, new Members, or those who have not previously signed, will be asked to complete this form to confirm their understanding and acceptance of the policy.

By signing the declaration below, I confirm that I have read and understood and will abide by the acceptable use conditions set out in the above named policy.

Member Full Name (print)	
Member Signature	
Date	

Once signed, please return this form to the Head of Democratic Services.

Document Control

Policy	ICT
Title	Elected Member Internet & Email Acceptable Use Policy
Author	Louise Evans, Data Protection & Improvement Officer
Owner	Service Director ICT & Digital Services
Initial Policy Launch Date	12.02.2018
Review date	This policy will be reviewed following any changes in legislation or working practices, and in any event, at least once every three years if no such changes occur.

Document Approvals

Major changes to this policy, such as amendments that alter its scope, introduce new obligations, or significantly impact Member responsibilities, must be approved by the Democratic Services Committee.

Minor amendments, which include non-substantive updates such as typographical corrections, formatting adjustments, or clarifications that do not change the intent or application of the policy, may be approved by the Chair and Vice-Chair of the Committee, with Members notified accordingly.

Version Control

Version No	Date Approved	Valid From Date	Valid To Date	Changes Made
1.0	Approved by Democratic Services Committee 12.02.2018	12.02.2018	2019	Re-write of Corporate policy to meet Elected Member needs / requirements.
2.0	Approved by Chair and Vice Chair, Democratic Services Committee	2019	10.09.2023	Minor Amends Amendments to wording; (6) Email disclaimer - removed reference to GCSX, (7) DPA 1998 to 2018. Amendments to job titles.
3.0	Reviewed by Democratic Services Committee	11.09.2023	12.07.2026	Minor Amends Review of policy to ensure fit for purpose.

4.0	Approved by Chair and Vice Chair Democratic Services Committee	13.07.2026	TBC	Full review by Data Protection Officer and Democratic Services. Refer to Democratic Service Committee reports and meeting 20th April 2026. Approved by Chair and Vice Chair of DSC 13.07.2026