RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

MUNICIPAL YEAR 2017/18

DEMOCRATIC SERVICES COMMITTEE	**AGENDA ITEM 4**
12TH FEBRUARY 2018	**UPDATED ELECTED MEMBER ICT, INTERNET & EMAIL ACCEPTABLE USE POLICY**

REPORT TO THE DEMOCRATIC SERVICES COMMITTEE

Author: Tim Jones, Head of ICT

1. PURPOSE OF THE REPORT

The purpose of this report is to:

1.1 Present a revised draft of the Elected Member ICT, Internet & Email Acceptable Use Policy to Members for consideration and approval.

2. RECOMMENDATIONS

It is recommended that Members of the Democratic Services Committee:

2.1 Review the changes made to the proposed Elected Member ICT, Internet & Email Policy (Version 1.0) as contained in Appendix I.

2.2 Approve the Elected Member ICT, Internet & Email Acceptable Use Policy (Version 1.0).

2.3 Agree the process for Elected Members to consent to the policy, as per the ‘Policy Acceptance Form’ contained within Appendix IV of the policy.

3. BACKGROUND

3.1 At the Democratic Service Committee held on the 11th September 2017 consideration was given to the Council’s Internet and Email Acceptable Use policy for use by Elected Members.

3.2 Following the feedback received from Members in respect of the policy, revisions have now been made that include clarification on the roles of Members that impact on the use of Council ICT equipment, internet and email facilities and the polices that support acceptable use.

3.3 In addition, to further support members in their understanding of their roles and responsibilities in particular in relation to data protection the Principal Information Management & Data Protection Officer will also be presenting Members with a data protection overview.

4. ELECTED MEMBER ICT, INTERNET & EMAIL POLICY

4.1 The Council considers the use of ICT equipment, internet and email to be a value asset that, if used correctly, Elected Members do their job more effectively. It is Council policy to promote its proper and efficient use.

4.2 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.

4.3 The overall purpose of these conditions is to:

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

4.4 The policy applies to Elected Members when using Council internet and email (@rctcbc.gov.uk) facilities to conduct official Council business.

4.5 Elected Members are expected to comply with this policy at all times when using the Council’s internet and email facilities, whether accessed locally or remotely (e.g. from a council office, Members home); and/or via any Council issued device (e.g. ipad, desktop computer, laptop, smartphone).

4.6 The policy is contained in Appendix I has been revised specifically for Elected Members taking into consideration the feedback provided by Members on the previous ‘corporate’ policy.

RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

ELECTED MEMBER ICT, INTERNET & EMAIL ACCEPTABLE USE POLICY

FINAL DRAFT Version 1.0

Document Information

Version:	Version 1.0
Status:	Final Draft (for approval)
Date:	February 2018
Owner:	Tim Jones, Head of ICT
Author:	Louise Evans, Principal Information Management & Data Protection Officer

STRONG HERITAGE | STRONG FUTURE
RHONDDA CYNON TAF
TREFTADAETH GADARN | DYFODOL SICR

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 do 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 the Council ICT equipment, internet and email facilities;
- protect the Council and its users from legal action, either civil or criminal;
- protect and safeguard information, and
- ensure compliance with relevant legislation.

2. SCOPE

Elected Members are likely to have three different roles:

i. They will act as a member of the council, for example as a member of a committee

ii. They will act as a representative of residents of their ward, for example, in dealing with complaints

iii. They may represent a political party, particularly at election time.

This policy applies to Elected Members when using Council ICT equipment, internet and email (@rctcbc.gov.uk) facilities to conduct official Council business – i.e. role i. above.

Elected Members are expected to comply with this policy at all times when using the Council's internet and email facilities, whether accessed locally or remotely (e.g. from a council office, Members home etc); and/or via any Council issued device (e.g. ipad, desktop computer, laptop, smartphone).

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, My Space) and content sharing websites (e.g. Flickr, Youtube). This is covered separately under the Council's Social Media Policy (see appendix III).

3. REASONABLE PERSONAL USE

Should they choose to do so, Members may use Council ICT equipment, internet and email facilities for reasonable personal use and/or when undertaking duties in relation to role ii. above provided it:

- 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, and
- 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 also use their Council email account (@rctcbc.gov.uk) within reason, in connection with any of the above activities.

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

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.

If using Council internet and email facilities when representing a member of the constituency (role ii. above) the Member should ensure that the constituent is aware of this, and that any email exchanges are subject to Council monitoring as outlined in Section 9.

Note: Any monitoring, review and access to such email messages sent from and received by a Member via their Council email account (@rctcbc.gov.uk) will be undertaken **strictly** to the extent permitted or as required by law, and as necessary and justifiable for legitimate Council business purposes.

4. ICT POINTS OF CONTACT

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

ICT Service Desk hours are:

- Monday – Thursday 08:00-17:30
- Friday 08:00-17:00

Contact details are:

- Tel: 01443 425080

- Email: ictservicedesk@rctcbc.gov.uk

5. TRAINING

Members must undertake appropriate ICT and Information Management training as part of their induction programme.

Additional individual training needs should be discussed with the Head of Democratic Services.

6. WELSH LANGUAGE ACT

Welsh is an official language in Wales and the public have a right to interact with the Council and its Members in Welsh - this includes communications sent/received via email.

To find out more about your responsibility under the Welsh Language Act please refer to the Councils 'Welsh Language Scheme' and 'Welsh Language Standards RCT'

7. 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.

8. EMAIL GOOD PRACTICE

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

9. MONITORING, AUDIT & ENFORCEMENT

The use of Council ICT equipment, 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.

- Council issued equipment, systems and any data held on them are the property of the Council.

- The Council reserves the right to access, monitor and review any Member's use of Council computer equipment, systems, facilities and data covered by this policy (and related Information Management policies) without the additional consent being required from the Member, and to bypass any security setting that a Member may make (e.g. password) subject to the authorisation of the Council's Monitoring Officer and Head of 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 as required by law, and as necessary and justifiable for legitimate Council business purposes, audit and security, or where there is reason to believe that a breach of security or a breach of policy has occurred (see section 10).

- The Council reserves the right to make and keep 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 computer 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.

10. 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'.

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 ICT equipment, 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 (role iii. above).

- 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 'Dignity at Work Policy'.

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

- Posting, forwarding or replying to chain letters or engaging in "spamming". (Spamming is the word used to describe the sending of 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 COUNCIL EMAIL GOOD PRACTICE (@rctcbc.gov.uk)

1. EMAIL ACCESS

All Members are allocated a Council email account in order to conduct Council business (role i. above). 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., to conduct **Council business**.

2. EMAIL ACCOUNT SECURITY

The Council's ICT section will provide Members with a network user id and password; this also controls access to a Members email account.

Members are responsible for their individual network and email account security and must take all reasonable precautions to prevent their account from being compromised.

3. ACCESS BY OTHERS

Members must not allow another person access to their email account unless that person is an employee of the Council and has a legitimate business need to access the account (e.g. a colleague requires access to the mailbox to monitor and respond to emails in the event of the Member being on leave).

Where access by another ('authorised') person is required, this must be provided through appropriate account security permissions. Members should contact the ICT Service Desk for further advice and guidance on how to do this.

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.

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 spam email 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 Councils 'Staying safe when using email' guidance which provides practical advice and information on some of the key things to look out for that act as warning signs of scams.

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 Councils Monitoring Officer and/or Head of Democratic Services.**

5. EMAIL MESSAGE SECURITY

Internal emails i.e. those sent between '@rctcbc.gov.uk' addresses 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 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 Council guidance 'Transferring personal information appropriately'.

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 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:

> 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, gan gynnwys negeseuon GCSX, 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
>
> 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 including GCSx 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

7. EMAIL CONTENT DISCLOSURE

Email messages sent and received in relation to official Council business may be disclosed under the Data Protection Act 1998, the Freedom of Information Act 2000, 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.

8. 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 'global' emails to mass recipients (i.e. emails to 75 recipients or more).

Should Members require a communication to be sent by email to a high volume of recipients this should be arranged via the ICT Service Desk.

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.

9. 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 identity.

10. 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 his / her 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.

11. 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 mail box 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.

Remember the Out of Office Assistant can be read by external organisations, so ensure your message is professional in its content and bilingual.

12. 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 Councils 'Email Etiquette' guide which is intended to promote a consistent and professional use of email etiquette across the Council.

APPENDIX III

RELATED POLICIES & PROCEDURES

1.	Investigating information security incidents & events	Incident Investigation.pdf
2.	Welsh Language Scheme	welshlanguagescheme.pdf
3.	Welsh Language Standards	WL Standards.pdf
4.	Dignity at Work Policy	Dignity at Work Policy - 2015.pdf
5.	Staying safe when using email	Staying safe when using email.pdf
6.	Transferring personal information appropriately	Appropriate transfer of Personal Information.pdf
7.	Email Etiquette	Email Etiquette.pdf
8.	Social Media Policy	Social Media Policy.pdf

APPENDIX IV

ELECTED MEMBER POLICY CONSENT FORM

Policy Name	Elected Member Internet & Email Acceptable Use Policy
Version Number	1.0
Date	TBC

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 the Head of Democratic Services.

Document Control

Policy	ICT
Title	Elected Member Internet & Email Acceptable Use Policy
Author	Louise Evans, Principal Information Management & Data Protection Officer
Owner	Head of ICT
Initial Policy Launch Date	TBC
Review date	This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Document Approvals

This document requires the following approvals:

1. Democratic Services Committee
2. Democratic Services
3. Information Management & Security Management Team

Version Control

Version No	Date Approved	Valid From Date	Valid To Date	Changes Made
1.0	TBC	TBC		Re-write of Corporate policy to meet Elected Member needs / requirements.