RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

MUNICIPAL YEAR 2015-16

DEMOCRATIC SERVICES COMMITTEE **24 MARCH 2016** **REPORT OF THE HEAD OF DEMOCRATIC SERVICES**	**AGENDA ITEM NO.2** **INTERNET & EMAIL ACCEPTABLE USE POLICY FOR ELECTED MEMBERS**

Author: **Ms.Karyl May, Head of Democratic Services**
Tel.No.01443-424045

1. PURPOSE OF THE REPORT

The purpose of this report is to inform the Committee of the feedback received from Members in respect of the Internet and Email Acceptable Use Policy.

2. RECOMMENDATIONS

It is recommended that Members of the Democratic Services Committee:

2.1 Note the comments made by Members (anonymised) as shown at Appendix 2 to the report;

2.2 Authorise the Head of Democratic Services and the Head of ICT to draft a further Internet & Email Acceptable Use Policy for elected Members only and that it be presented to this Committee for consideration.

3. BACKGROUND

3.1 Members will recall that at the last meeting of this Committee held on the 26th November, 2015, consideration was given to the Internet and Email Acceptable Use Policy for Elected Members (copy of policy shown at Appendix 1).

3.2 Following the views expressed at that meeting, Members agreed that the matter be deferred to allow **all** Members to be given the opportunity to comment on the policy by the 30th January, 2016 and a report thereon be presented to this Committee.

3.3 Emails together with the policy were sent to all Members on the 1st December, 2015 and further reminders were sent on the 5th and 20th January, 2016.

3.4 Attached at Appendix 2 are the comments received from Members (anonymised), where the Committee will note that there is a mixed reaction to the policy.

4. CONCLUSION

4.1 In view of the mixed response of Members in respect of the policy, it is recommended that Officers look at redrafting the policy to take into consideration the comments made and a further report and policy be presented to this Committee in the near future for consideration.

APPENDIX 1

RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

INTERNET & EMAIL ACCEPTABLE USE POLICY

Version 2.2

Revised and effective from 26th November 2015

Document Control

Policy	ICT
Title	Internet & Email Acceptable Use Policy
Author	Leigh Gripton
Filename	Internet and Email Acceptable Use
Owner	Director of Customer Care & ICT
Subject	Internet & Email Acceptable Use
Protective Marking	Official
Review date	The Information Management Executive Group will formally review this policy on at least a 6 monthly basis.

Revision History

Revision Date	Reviser	Previous Version	Description of Revision
01/04/2014	Leigh Gripton	1.2.2	Final - updated re: social media policy cross reference and auto-forwarding of e-mails.
08/08/2014	Leigh Gripton	1.2.3	Final - updated re: Government Protective Marking Scheme
02/02/2015	Leigh Gripton	1.2.4	Draft - updated re: Schools Addendum.
07/07/2015	Leigh Gripton	2.0	Final - updated re: social media, e-signatures, PSN e-mail users & Cloud Storage.
25/08/2015	Leigh Gripton	2.1	Final - Headteacher acceptance form added.
26/11/2015	Leigh Gripton	2.2	Final - Elected Member acceptance form added. Subject to Democratic Services Committee approval.

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Information Management & Security Executive Group	Chair: Leigh Gripton (SIRO) and Director of Customer Care & ICT	Subject to Democratic Services Committee Approval 26/11/2015

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
All Employees and Elected Members plus (Contractors & third party suppliers, where appropriate via lead Council officers)		

INTERNET & EMAIL ACCEPTABLE USE POLICY

CONTENTS

1. Introduction

This policy applies to the use of Internet and/or Email access provided by the Council and is applicable to all Council users, including Elected Members, staff, contractors, consultants, visitors, authorised third party users and any other authorised users who access these Council Information Systems from network connected sites or remote locations.

Note: Sections 5.9, 5.10 and 5.24 of the Policy are not applicable to Elected Members at this time.

2. Purpose of Internet & Email Acceptable Use Policy

2.1 The purpose of this document is to set out the Council's policy on the access and acceptable use of its Internet and Email facilities.

2.2 The Council considers the Internet to be a valuable asset that, if used correctly, can help Council users do their job more effectively. Therefore it is Council policy to promote its proper and efficient use.

2.3 Conditions of use (including legal and regulatory matters) are detailed later in this policy but the overall purpose of these conditions is to:

- protect the Council and its users from legal action, either civil or criminal;
- protect the Council and its partners from embarrassment and public allegation;
- promote efficient and safe use of the Council's Internet and Email facilities; and
- avoid dispute between users, the Council and members of the public.

2.4 The ICT Information Management & Security Executive Group will review this Internet & Email Acceptable Use Policy every six months, and re-issue for consent annually, drawing attention to any material changes that may have been made.

3. Scope of Policy

3.1 This policy defines what the Council considers as acceptable use of its Internet and Email facilities and sets out rules and guidelines for the access and use of these facilities.

3.2 The policy does not include guidance on the acceptable use of Social Media such as blogs, message boards, social networking (Facebook, Twitter, LinkedIn, My Space) and content sharing websites (Flickr, Youtube). This can be found separately under the Council's Social Media Policy.

3.3 It applies whenever they are logged on under their Rhondda Cynon Taf provided User ID and whether they are accessing the system directly via the Council's network, using a home Internet connection, an Internet café, an external Web-based Email system, a mobile phone, or any other method used where a user logs on under this User ID.

3.4 All communications sent, received or created within Council systems, together with any information stored on Council systems, are the property of the Council and as such cannot be considered as private and may be checked in accordance with the law.

3.5 All users must agree to read, understand and comply with the terms and conditions of this policy.

4. Management Policy

4.1 The Council reserves the right to examine any personal files stored on the Council's systems, this includes the contents of any files, Email or other electronic communications sent to the user. Council systems are primarily for the storage of work related material.

4.2 The ICT Service will produce reports monthly, detailing the Internet pages users have accessed and these can be provided to Service Directors \ Head of Service for review for both statistical purposes and to ensure compliance with this policy.

4.3 The Council reserves the right to monitor, access and review any individuals use of Council Computer equipment, systems and facilities covered by this policy (and related policies e.g. The Council's Information Security Policy) without the additional consent being required from any user. Monitoring will be undertaken for the purpose of business operations, audit and security or where there is reason to believe that a breach of security or a breach of policy has occurred.

5. Conditions of Internet & Email Use

5.1 Users should primarily use the Council's Internet and Email facilities for business, team building and career development activities.

Reasonable personal use is acceptable provided it :

- is undertaken in a user's own personal time or a members own personal time;
- does not interfere with the performance of your official duties;
- does not take a priority over your 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.

5.2 In accordance with the Council's Information Security Policy and Password Management Policy all users are issued with a permanent logon User ID and initial password, which they are compelled to change at least every 60 days,

this allows a user certain permissions, e.g. access to the Internet and Email facilities and access to specific drives and applications.

5.3 Users are responsible for their individual accounts and as such they should take all reasonable precautions to prevent others from being able to use their account.

5.4 Personal passwords must not be written down, nor physically or electronically stored by the user.

5.5 Users must not use anyone else's password and must not directly / indirectly divulge their passwords or those of any groups that they belong to.

5.6 Do not send system account information by Email, unless authorised by ICT; this includes user accounts, passwords, internal network configurations, addresses or system names. This information is confidential.

5.7 Users must not manually or automatically forward Council work related emails, that contains personal or sensitive (including commercially sensitive) information, to their own personal/home email account, e.g. Googlemail, Yahoo, Hotmail etc. This is strictly prohibited.

5.8 The automatic forwarding of Council emails to internal (i.e. @rctcbc.gov.uk) email accounts is permitted, subject to approval by the relevant line manager and ICT.

5.9 Should users have a legitimate business need to access work related emails and/or Council systems from home, remote access may be arranged formally via the ICT Service Desk, subject to approval of the relevant business case by the user's line manager.

5.10 Should any user require secure e-mail send/receive facilities for external communications, for sensitive information sharing please contact the ICT Service Desk who will be able to support you with your request.

5.11 Before sending emails that contain personal information users must consider the guidance contained within the 'How To' Guide: Transferring personal information appropriately to ensure that most appropriate method of communication has been selected.

If email is the most appropriate method of communication for transferring the data, when sending the email, users must adhere to the good practice advice contained within the guidance for reducing the potential risks associated with emailing personal data e.g. email being sent to the wrong recipient or wrong attachment being sent.

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 is

recommended. Users should discuss their requirements with their Line Manager and contact the ICT Service Desk for further advice and guidance.

5.12 Users must check their Emails frequently; any that need to be kept should be saved in a relevant folder or on a shared drive, while those that are no longer required should be deleted.

5.13 Users access to, and the use of non endorsed "cloud storage & facilities" e.g. Dropbox & Google Docs, is not allowed unless approved by ICT. For those facilities where approval has been granted by ICT, **any use of such cloud facility must not be used for the purpose of storing or sharing confidential, personal or sensitive information**.

5.14 When downloading electronic files, users must follow the computer virus protection procedures as set on your Council computer, helping to avoid the inadvertent spread of computer viruses. ICT staff will update these periodically.

5.15 Computer viruses are a type of software that can be transferred between programs or computers without the knowledge of the user, they contain instructions as to when to activate and what to do, e.g. displaying annoying messages, deleting files or infecting other programs. Many do no lasting damage but some can cause serious problems for the Council and they all constituent a breach of security.

5.16 If you suspect you have been the victim of a computer virus, or become aware of the presence of a computer virus - this includes any verbal communication you may have received from an external body - you should not under any circumstance send or forward any further Emails to any colleagues. Contact the ICT Service Desk by telephone immediately in such circumstances.

5.17 If you are informed of the presence of a hoax virus, do not make colleagues aware by any electronic means, as by doing so you may inadvertently spread the virus. Contact the ICT Service Desk by telephone immediately in such circumstances.

5.18 If users mistakenly access inappropriate information, they must immediately advise their Line Manager and report the incident to the ICT Service Desk. This will protect them against any claim that they have intentionally violated this policy. Elected members must report the incident to the Council's monitoring Officer (or his delegated officer).

5.19 Users must promptly disclose to the ICT Service Desk any messages or images they receive that are inappropriate or make them feel uncomfortable. The ICT Service Desk will advise on what action to take.

5.20 **Users may not use the Internet & Email at anytime for example for:**

- 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.

- Accessing material that is profane or obscene (pornography), that incites illegal acts, violence or discrimination towards other people (hate literature).

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

- When sending commercially confidential information to external bodies, you must respect the Council's Finance Procedure and Contract Procedure Rules.

- Online gambling.

- 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.

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

- Engaging in personal attacks, including prejudicial or discriminatory to other people.

- 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 (2015).

- 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).

- Officers will not 'speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council), unless authorised to do so.

- In order to maintain system resources, users must not download large files unless absolutely necessary. If it is necessary, they should download the file at a time when the system is not being heavily used and immediately remove the file from the system on finishing with it. If you are expecting an Email attachment, which you anticipate will be larger than normal, contact the ICT Service Desk for advice.

- The downloading of business applications, operating system upgrades and other programme files is strictly prohibited (ICT staff excepted), unless they are available on the Intranet or the Council's Website.

- **Those Council Officers who may be required to undertake any of the prohibited actions set out in 5.20 (either as part of the Council's monitoring regime or in relation to their official duties), are required to seek prior written authorisation from their Head of Service and the Head of ICT). Elected Members would need to seek authorisation from the Council's Monitoring Officer (or his delegated officer).**

5.21 **Acceptable personal use**

Users may use the Council's Internet and Email facilities for reasonable personal use. Reasonable use of the Council's Internet and Email facilities is only permitted during a user's personal time. i.e. before or after work, during lunchtime and is subject to users clocking\signing out. Users should note that this is a privilege and not a right, which can be removed at any time.

For additional clarity please refer to the Council's Flexi-time Working Hours Policy.

5.22 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 and Web Based Email services e.g. MSN and Hotmail. All such use is carried out at users' own risk and the Council does not accept responsibility or liability for loss caused as a result of use of the Internet.

The conditions of use set out in the **Section: 5.20** apply equally to the personal use of the Council's Internet and Email facilities.

5.23 Users are reminded that all Internet and Email activity is monitored and traceable at all times, therefore remember that when you are accessing the Internet and Email facilities for personal or business use, any activity will be logged via Council ICT systems.

5.24 **PSN e-mail users ONLY**

- Any Council users that are Public Service Network (PSN) email users must read, understand and sign the PSN Acceptable Usage Policy and Personal Commitment Statement. Please contact the ICT Service Desk for additional support and guidance.

- PSN email users must use the Central Government Cabinet Office's Government Protective Marking Scheme when communicating with Central Government bodies e.g. Department of Work & Pensions.

6. Monitoring and Enforcement

6.1 All communications and stored information sent, received, created or contained within the Councils ICT systems are the property of the Council and accordingly should not be considered as private and may be checked in accordance with the law. The Council reserves the right to bypass any security setting that an user may make, in order to protect the Council's interest.

6.2 Details of all Internet and Email activities leave an 'electronic footprint' on both personal computers and the Internet servers. The ICT Service will produce monthly reports detailing usage activity and these will be provided to Service Directors \ Heads of Service for review, for both statistical purposes and to ensure compliance with this policy.

6.3 **The ICT Service may undertake Internet & Email monitoring periodically and without notice for the following purposes:**

- To help maintain compliance with regulatory or self-regulatory practices.

- To provide local Service management with usage statistics and reports to assist with the day-to-day management of their services. (It is the responsibility of each local Service manager to assess the provided reports).

- To support local service managers in the interpretation of usage statistics and reports. It is the responsibility of each local manager to use the provided reports to monitor the usage of their users and enforce the usage policy.

- To establish facts and protect the interests of the Council and its users.

- To prevent unauthorised use of the Council's ICT systems.

- To prevent inappropriate/offensive media from entering the workplace.

- To assist with any investigation whether internal or by externally authorised investigating authorities (e.g. Police, Internal or External Audit).

- To comply with the Council's access to information obligations under the Data Protection Act 1998 and the Freedom of Information Act 2000 or any statutory modification under such acts.

6.4 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.

6.5 The Council reserves the right to place restrictions on the use of Internet and Email accounts at any time.

7. Consequences of Breach to Policy

7.1 Any breach of this and related policies may warrant further investigation that may lead to the Council's disciplinary procedures being invoked and in certain circumstances, may necessitate the involvement of the Police.

7.2 The Council will co-operate fully with any Audit or Police investigation. If the investigation demonstrates that material that is accessed is offensive, e.g. pornographic, advocate's illegal acts, violence or discrimination to other people, this will be considered gross misconduct and appropriate disciplinary procedures will be followed, possibly resulting in dismissal.

8. Reporting Security Events (Breach of Controls)

8.1 Any employee or computer user of the Council who considers that this policy has not been or is not being followed by any user in respect of Email or Internet usage, the results of which could be damaging to other staff, users, the Council, or illegal in any way, are encouraged to raise the matter with their Line Manager, or Head of Service and follow the Information Security Incident Management Policy. Elected Members are encouraged to raise the matter with the Council's Monitoring Officer (or his delegated officer).

8.2 If any potential breach of these rules comes to the attention of Service Managers, management should in consultation with Human Resources instruct ICT Services and or Internal Audit to investigate further. It will be for Service Managers in consultation with Human Resources to consider whether disciplinary action in accordance with the Councils disciplinary procedures is appropriate.

8.3 All users or agents of the Council will be encouraged to report any security event, actual or potential, without fear of recrimination. Every effort will be made to learn lessons from security events in order that preventative controls may be put in place for the future.

8.4 Where an employee or computer user of the Council inadvertently makes a genuine mistake or the unexpected occurs it should be reported to their Line

Manager or the ICT Service Desk. Elected Members are asked to report such incidents to the Council's Monitoring Officer (or his delegated officer).

9. Compliance with Legislation and Regulation

9.1 Users should note that an Email has the same significance and legal implications as a signed letter. Furthermore users should never send 'off the record' Emails – nothing is 'off the record' where the law requires disclosure of information.

9.2 Messages sent via the Email system can give rise to legal action against the Council. Claims of defamation, breach of confidentiality or contract could arise from the misuse of the system.

9.3 Emails must never contain what could be considered as a defamatory statement, i.e. one that may possibly damage the reputation of another individual or company. Remember that damaging Emails may have to be disclosed in litigation or in investigations by other councils or organisations. Users are also reminded that messages can be disclosed in any legal action commenced against the Council relevant to the issues set out in the Email.

9.4 It is recommended that user do not transmit / receive graphical images or scanned signatures either as an attachment or embedded as a signature to Emails. These graphical files could easily be copied and applied fraudulently to other documents e.g. faxes or electronic letterheads.

9.5 Users will respect the rights of copyright owners. Copyright infringement occurs when items protected by copyright are inappropriately reproduced. Where items contain conditions regarding their use, these should be followed. Users should request permission from the copyright owner if they are unsure as to whether or not such items can be used.

9.6 Users should be aware of UK and international laws that govern the use of Emails. These include any statutory modifications or amendments but are not limited to:

- Copyright
- Libel and Defamation
- Public Records Acts 1958 and 1967
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Electronic Commerce (EC Directive) Regulations 2002

10. General Email Responsibilities

10.1 Email Housekeeping

- Good practice is that you should save the Email in the relevant folder on a personal or preferably a team shared drive. This brings together all documents relevant to a theme or activity and will make it easier for you or your colleagues to search for work-related Emails and related documents.

- Add to or amend the original subject line if this helps with filing. Delete all Emails that do not need to be saved as soon as possible.

- The Council has set a limit on the size of mailboxes, which includes Inbox, Sent Items and Deleted Items, and once the limit is reached a user will not be able to send or receive Emails. It is the responsibility of each individual to manage his / her mailbox. The owner of the inbox 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. Users 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.

- Create folders for Email categories, people, services, sections etc.

- Create archive files on PC hard disk to enable transfer of old Email messages from the central server to your PC (contact ICT Service Desk for help and guidance with this).

10.2 Email Etiquette

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

- Users must ensure that they adhere to the Councils 'How To' Guide: Email Etiquette which is intended to promote a consistent and professional use of email etiquette across the Council.

- If you accidentally receive someone else's Email, you should return it to the original sender explaining that you have received it in error.

- Use the "Out of Office Assistant" if you know you will not be able to access your Email system 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.

- Do not send non-work related Emails to large numbers of people who have not agreed to receive them, even if the contents may appear to be of interest. This is sometimes known as spam, bulk, chain or junk mail.

- The ICT Service provides central systems to block unwanted or spam Email. These automated systems provide a high level of protection, however these systems are not 100% fail safe and it maybe possible for spam mail to be received. Under this circumstance it is the responsibility of users that receive them to deal with them, in consultation with the ICT Service Desk.

- If spam Emails are received, consider: Is it from a known person or company? Was the Email requested by providing your details on a website or on a paper form? Does it contain useful information relevant to your work or the Council's business?

Appendix I

RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

Elected Members Policy Acceptance Form

Policy Name	Internet & Email Acceptable Use Policy
Version Number	Version 2.2
Date	Revised and effective from 26 November 2015

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.

In relation to Section 7 of the policy, I further understand that any violation of this policy may result in ICT access privileges being revoked and possible disciplinary action being taken against me, in accordance with the Council's Members Code of Conduct.

Note: Sections 5.9, 5.10 and 5.24 of the Policy are not applicable to Elected Members at this time.

Full Name (print)	
Network User ID	
Signature	
Date	

APPENDIX 2

INTERNET AND ACCEPTABLE USE POLICY FOR ELECTED MEMBERS

Following the meeting of the Democratic Services Committee held on 26th November, 2015, the following comments have been received from Members in respect of the ICT/Email Policy:-

Date	Comments
06.01.16	I have read the Policy and I am happy with it.
02.12.15	I'm happy with the content of the policy and have no comments to make/add.
21.01.16	Could I just say that I use the computer for emails and letters mainly to my constituents, I have taken on board all that has been suggested and will abide by them.
06.01.16	I agree with the attached policy
01.12.15 06.01.16	I am shocked by the proposal to restrict councillors from using the lap tops for reasons in the report councillors are on call 24/7 365 days of the year constituents contact us at unbelievable times if their needs are of an urgent nature but except for now I have never complained and sure none of my colleagues have ever complained. If I cannot use my lap top for an occasional holiday the Council can come and collect my PC whenever they wish. I have not changed my views on this decision and you can now supply all my correspondence and salary information by post you can now remove my PC as soon as you like.
12.01.16	This looks ok to me.
08.12.15 email to L.Gripton	It occurs to me that the draft document that we discussed at the Democratic Services Committee is very, very full in telling everyone what they should not do. I wonder if there could be a section which tells Councillors what they can do: i.e. They can use a RCT computer to hold a non RCT e.mail address and conduct non RCT correspondence. They can use a RCT computer to undertake political and other work activities so long as they do not do this through their RCT email address
22.01.16	I would like to submit the following observations and concerns. They are matters that I first raised with Mr.Leigh Gripton in August of 2014 when he sent me a draft copy. My understanding following those exchanges was that there would be no issue with manually transferring all email exchanges to my private email address. I reminded Mr.Gripton that all Members are registered as data

	controllers with the Information Commissioner and that these registrations are renewed on an annual basis by the Corporate Governance unit within Legal and Democratic Services. Members are also made aware of the penalty for non compliance. I would like clarification on this matter because the practical ways that Members manage their work doesn't seem to be acknowledged or provided for in full in para 5.7 of the policy document. Para 5.20 mentions political lobbying but I cannot trace any reference to the fact that the system should not be used for Party Political reasons. Given that it is an offence to use publicly funded resources for Party Political reasons and is a breach of the Members Code of Conduct I wondered how this will be made clear in this Policy document. I know there is a separate Social Media Policy for it is mentioned at para 3.2 and that the Internet and Acceptable Use Policy for Elected Members does not include guidance on the acceptable use of Social Media. I am unfamiliar with the detail of the Social Media Policy what I am aware of is that Members use if tor Party Political purposes. How does this square with the Council's right to vet the appropriateness of those exchanges.
06.01.16	No comments from me other than to say that upon reading the document, I think that most areas of the online sphere are covered and the guidance provided is instructive and sufficiently robust.
06.01.16	Seems a good policy to me covering all aspects.
05.01.16	I am a little concerned with section 4 item 4.1 to 4.3 also 6.1 is similar – if I have casework on my laptop or have used my council email address to converse with a constituent about a problem they have then this information has to be confidential between myself and the constituent in the carrying out of my duty as a ward councillor, so this information should not be liable for inspection by the council without the express permission of the constituent otherwise we as councillors are breaking the data protection rules as data controllers. 5.7 is not practical as I can open emails on my phone but can't see complex information or print the email out without forwarding it to my work computer via yahoo or parliament in order to print it to look at. I am happy with the rest but very concerned that if we as elected members sign the declaration as it stands then the sections noted above may prevent us from doing our jobs as ward councillors and keeping the confidentiality expected when constituents bring their problems to us in casework.

25.01.16	This policy is clearly designed for employees with the elected members tag just bolted on. That is entirely inappropriate as elected Members are NOT Council employees but representatives of the people in their ward and beyond. Our roles and responsibilities are completely different and our first loyalty is to the people not the Council. I especially object to the following sections: 4. Management Policy 4.1 ***The Council reserves the right to examine any personal files stored on the Council's system,*** *this includes the contents of any files, Email or other electronic communications sent to the user. Council systems are primarily for the storage of work related material.* 4.2 ***The ICT Service will produce reports monthly, detailing the Internet page users have accessed and these can be provided to Service Directors/Head of Service for review*** *for both statistical purposes and to ensure compliance with this policy.* 4.3 ***The Council reserves the right to monitor, access and review any individuals use of Council Computer equipment, systems and facilities covered by this policy (and related policies e.g. The Council's Information Security Policy) without the additional consent being required from any user.*** *Monitoring will be undertaken for the purpose of business operations, audit and security or where there is reason to believe that a breach of security or a breach of policy has occurred.* What would be classed as "personal" files? Any files sent to me in my capacity as a Councillor are personal. The people of my ward and indeed the wider area email me to what they believe is a confidential email address not one which can be randomly accessed by a Council employee. Who exactly would be doing this "examining" of files on behalf of "the Council" and which Service Director/Head of Service would be reviewing reports? Where is their remit to do this? And indeed who employs them to do it? All in all this policy smacks of a North Korean Big Brother mentality and one that surely flies in the face of the data protection regulations this policy claims to be in place to protect.

	Looking form a slightly different angle, who monitors the accounts of Chief Officers? What about the Chief Executive? There are surely privacy issues here. I wonder if I would be given the posers by a Kim Jong Un character to access his Chief Officers email accounts? If you are intent on pressing ahead with this policy then please alter my contact details on the RCT Council website to give an alternative email address where residents can contact me in the full knowledge that it will not be liable to snooping by "officers" of the council. That being so I would therefore require the following email address to be placed on all council literature and electronic web pages for people or whistleblowers to contact me without the fear of some "monitoring" or "examination" by an "officer of the council" ***(EMAIL ADDRESS DELETED as information to be kep anonymised)*** **5.7** *Users must not manually or automatically forward Council work related emails, <u>that contain personal or sensitive (including commercially sensitive) information,</u> to their <u>own personal/home email account,</u> e.g. Googlemail, Yahoo, Hotmail etc. This is strictly prohibited.* Members are already subject to a Code of Conduct as well as the Data Protection Act and other regulations and so forwarding emails to another personal account should not be viewed as a breach of security. Because of personal doubts over security, which have been in some way supported by the suggestion that our email accounts could be monitored, I prefer to respond to residents who contact me via my personal email accounts. Also, unless I have missed something, there does not appear to be anything in this policy which says we cannot forward to anyone else's personal accounts. One would hope that this is surely an oversight, but one that would have had dire consequences had it been perpetrated in Pyongyang. Alternatively it may well be there to allow "officers of the council" to forward emails to outside bodies or indeed non-members of the council such as school governors etc.? Indeed when Cllr.Christopher, the then Cabinet Member and Deputy Leader of RCTCBC referred in a council meeting to items contained in an email exchange between myself and the then director of highways I was told by the presiding legal officer that as a cabinet member with the Highways portfolio he is given access to all such correspondence, a practice that sill continues today?

	5.20 <u>Users may not use the Internet & Email at anytime for example for:</u> *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.* Absolutely 100% agree that Council resources should not be used for political purposes although this should be for ANY political lobbying or purpose not just that which seeks to achieve a political result that is against Council policy or goals." No group or individual should use Council emails or other resources e.g. the website, or the Council press team to promote their political goals or the electoral ambitions of themselves or party colleagues. In fact I have had cause to complain about this sort of behaviour in the past. Therefore if there is to be a "free society" IT policy for Members then I would like to see this section enhanced and extended within it. **6. Monitoring and Enforcement** **6.1 *All communications and stored information sent, received, created or contained within the Councils ICT systems are the property of the Council and accordingly should not be considered as private*** *and may be checked in accordance with the law. The Council reserves the right to bypass any security setting that a user may make, in order to protect the Council's interest.* **6.3 *The ICT Service may undertake Internet & Email monitoring periodically and without notice.*** I am sure residents contacting their Councillors would be dismayed to know that their communication was not "considered as private." And just who is going to "check" these emails and what are they checking for? This appears to be a gross breach of data protection. This to "protect the Council's interest" but what about the people who are supposed to be served by the Council, the electorate, surely we answer them first? If there is to be an IT and email policy for elected members then it needs to be rewritten from scratch. I am not prepared to sign up to a policy that gives carte blanche to un-named people acting for "the Council" to

	spy on what should be private correspondence between residents and myself. I am elected to represent the people not the Council. Oh, and I bet there will not be any trustworthy and openly verifiable method of auditing which "officer of the council" checked whose emails for what and that states when they were checked and why. Or will there?
24.01.16	My main concern is regarding the use of social media. I think there is always a danger of failing into difficulties with it if used by individual Councillors. Of course that is for individuals to consider. I for one will steer clear. I do think however that being able to use smart phones and ipads for email is brilliant and saves a great deal of time.
06.01.16	Looked at policy and all seems standard procedure. No comment to make. From my own point – I must make sure I follow the housekeeping rules and keep files tidy.
12.01.16	I have no problem with the policy.
06.01.16	I've read the policy and would make two comments: 1. Why is it necessary to consent to the whole policy when it is only a revision, surely a consent to those would be adequate (2.4). 2. To whom would monitoring reports vis a vis Councillors be forwarded? (4.2)
24.01.16	The policy looks fine; no further comment to make. When will you need the acceptance form; or does it have to go back to Committee first?
05.01.16	The policy as per the above is quite straightforward. I don't foresee any problems.
20.01.16	It looks pretty sensible to me. Not much more I can say.