COUNCILLORS EMAIL, INTERNET, TABLET AND TELEPHONE ACCEPTABLE USE POLICY

PURPOSE OF REPORT

1. To present the updated and amended councillors email, internet, tablet and telephone acceptable use policy for consideration and approval.

RECOMMENDATION(S)

2. That the updated and amended policy, presented with this report be approved and adopted.

EXECUTIVE SUMMARY OF REPORT

3. The existing “Members’ E-Mail, Internet and Telephone Acceptable Usage Policy” presented to Executive Cabinet on 7 January 2010 is now out of date due to changes in technology and working practices.

The updates and amendments to the policy include:

   a. specific reference to the use of tablet devices
   b. note of Wi-Fi access in the main council buildings
   c. information relating to 3G or higher mobile ultra-broadband internet access
   d. reference to the use of smart phones
   e. recognition of mobile and home working by councillors
   f. confirmation that paper agendas and reports will no longer be sent by post.

REASONS FOR RECOMMENDATION(S)

(If the recommendations are accepted)

4. The updated policy
   
   • is in line with aims set out in the council’s digital strategy
   • forms part of the council’s information security framework
   • should be available for signing by all councillors on receipt of a tablet device or at a review appointment
ALTERNATIVE OPTIONS CONSIDERED AND REJECTED

5. No viable alternative options have been identified.

CORPORATE PRIORITIES

6. This report relates to the following Strategic Objectives:

| Involving residents in improving their local area and equality of access for all | A strong local economy |
| Clean, safe and healthy communities | An ambitious council that does more to meet the needs of residents and the local area |

BACKGROUND

7. As outlined in the Executive Cabinet report of 16 January 2014 the implementation of new technology and use of tablet devices will enable council members to access information on the move, take advantage of secure Wi-Fi access in the main council buildings and contribute to the reduction in paper and printing costs outlined in the council’s digital strategy plans.

8. The drive for efficiencies has led to improvements in digital systems across the council and the roll out of tablet devices for councillors will improve access to these systems.

9. Changes in technology and working practices prompted a review of the current acceptable use policy which was approved by the monitoring officer on 12 June 2014 and strategy group on 24 June 2014.

10. A revised policy document relating to officers acceptable use will be presented at a later date.

IMPLICATIONS OF REPORT

11. This report has implications in the following areas and the relevant Directors’ comments are included:

| Finance | Customer Services |
| Human Resources | Equality and Diversity |
| Legal | Integrated Impact Assessment required? |
| No significant implications in this area | Policy and Communications |

COMMENTS OF THE MONITORING OFFICER

12. No comments on this report.

COMMENTS OF THE HEAD OF POLICY AND COMMUNICATIONS

13. As outlined in the report, the acceptable use policy is in line with the council’s other related policies, in particular the information security framework and the council’s digital strategy.

Lesley-Ann Fenton
Director Customer and Advice Services
Following careful consideration and assessment of the contents of this report, I approve the recommendation(s) contained in Paragraph 2 of the report in accordance with my delegated power to make executive decisions.

Councillor Graham Dunn
Executive Member (Customer and Advice Services)
COUNCILLORS EMAIL, INTERNET, TABLET AND TELEPHONE ACCEPTABLE USE POLICY – MAY 2014

FOREWORD

The aim of this policy is to protect the council and protect you. Please take time to read it.

It is closely linked to the corporate Information Security Framework which details how councillors and employees must work to ensure we maintain the security of our information assets.

Although the framework considers wider security issues, it recognises the key role this document plays in supporting us all to secure our workplace.

The council is also obliged to conform to national security standards including Public Services Network (PSN)

A separate policy specifically relating to the use of council issued tablets is included with this document at Appendix A

This policy:

- Sets out general rules for the acceptable use of digital systems
- Points out that the way we use the facilities made available to us reflects on the council.
- Reminds us of our responsibilities to handle personal and sensitive information properly and that customers'/constituents’ e-mail addresses themselves may be personal information
- Requires users to contact ICT services before sending confidential or sensitive information via email
- Describes how and when personal use of e-mail and internet is permissible
- Requires us to remove personal e-mail from the council’s systems
- Prohibits the use of council e-mail addresses on public websites for non-business purposes
- Sets out the circumstances in which the council may monitor communications.

If you need clarification of anything in this policy please ask your group leader and/or the monitoring officer.

Gary Hall
Chief Executive
1 July 2014
1. OVERVIEW

1.1 INTRODUCTION

Communication plays an essential role in the conduct of the council’s business. How you communicate with people not only reflects on you as an individual but also on the council as a whole. In some cases the council will be legally liable for statements made or actions taken through its communication facilities.

We value our ability to communicate with colleagues, customers, councillors and partners and the council invests substantially in information technology and communications systems which enable you to do so more efficiently. We rely on you to use those resources responsibly and this policy sets out the council’s requirements.

1.2 WHO DOES THIS POLICY APPLY TO?

This policy applies all councillors, using the council’s ICT equipment or systems.

1.3 WHAT FACILITIES DOES THIS POLICY COVER?

The facilities covered by this document include access to all communication facilities provided by the council including internet and e-mail services, telephones, instant messaging, copiers and scanners.

1.4 PERSONAL USE OF FACILITIES

The council’s communications facilities are provided for the purposes of council business. A certain amount of limited and responsible personal use by users is also permitted.

1.5 WHAT HAPPENS IF THE POLICY IS BREACHED?

If our rules and procedures are not followed, then use of the council’s facilities may be curtailed or withdrawn. Serious breaches of this policy may amount to a breach of the Code of Conduct and the withdrawal of permission to use the council’s equipment for personal purposes.

Some aspects of this policy also deal with matters which amount to criminal offences under the Computer Misuse Act.

If there is anything in this policy that you do not understand, please ask for clarification.

2. GENERAL PRINCIPLES

2.1 You must use the council’s information technology and communications facilities sensibly, professionally and lawfully. You must use them with respect for your colleagues and for the council and in accordance with this policy and any other relevant rules and procedures.

2.2 We regularly deal with personal information or with our own or partners’ confidential or sensitive information. While the council strives for openness in its dealings you must treat information which we hold with utmost care.
2.3 Modern communication facilities and particularly the internet allow for easy copying of material. Please remember that most material on the internet belongs to someone and reusing it may breach their copyright.

2.4 Particular care must be taken when using e-mail. E-mail can be produced in court in the same way as other kinds of written statements. You can enter contracts, bind the council to certain action or defame a third party by e-mail in just the same way as you can by letter and so create liabilities both for the council and for you personally.

2.5 All messages sent externally using council systems should demonstrate the same professionalism as that which would be taken when writing a letter. For some internal purposes the council accepts that the style of correspondence may be less formal. However, you should remember that e-mail may have to be disclosed in legal proceedings or in response to a request under the Data Protection Act or Freedom of Information Act. The golden rule is therefore never to send a message which would embarrass you or the council if it became public.

2.6 Under no circumstances should users communicate material, either internally or externally, which is defamatory, obscene, or breaches the council’s equal opportunity policies.

3. USE OF ELECTRONIC MAIL

3.1 GENERALLY

3.1.1 Users should note that a disclaimer is added automatically to all external e-mail sent by the Council.

3.1.2 Do not amend any messages received and, except where specifically authorised by the other person, do not access any other person’s in-box or other e-mail folders nor send any e-mail purporting to come from another person.

External e-mail is not a secure form of communication. It is easy to send e-mail to the wrong person. In addition once e-mail has left the council’s systems it is susceptible to interception.

For that reason, if you need to send confidential information or personal information which could cause distress if disclosed you should contact ICT Services and ask for the e-mail to be encrypted. It is, in any event, good practice to re-read and check an e-mail before sending and to confirm that you are sending the e-mail to the right person.

3.1.3 If you copy an e-mail to others, it may breach the Data Protection Act if it reveals all the recipients’ e-mail addresses to each recipient. This is most likely to apply in the case of mailing lists and similar sent to external parties. It could though apply if internal e-mail is being sent relating to personal rather than work matters.

3.1.4 In these cases it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an e-mail to more than one recipient. If in doubt, seek advice.

3.2 BUSINESS USE
3.2.1 If the e-mail message or attachment contains information which is time-critical, bear in mind that an e-mail is not necessarily an instant communication and consider whether it is the most appropriate means of communication.

3.2.2 If you have sent an important document, always telephone to confirm that the e-mail has been received and read.

3.2.3 In light of the security risks inherent in some web-based e-mail accounts, you must not e-mail business documents to your personal web-based accounts. You may send documents to a customer’s web-based account if they have asked you to do so.

3.3. PERSONAL USE

3.3.1 Although the council’s e-mail facilities are provided for the purposes of council business, you may occasionally want to use them for your own personal purposes. This is permitted on the condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of council facilities for personal correspondence, you can expect very little privacy because the council may need to monitor communications.

3.3.2 Under no circumstances may the council’s facilities be used in connection with the operation or management of any other business or for commercial activity. The facilities should also not be used by councillors for general party political activity and, in particular must not be used for campaigning or election activities. They may, however, be used for correspondence within the political group, general political research, casework as a councillor and similar activities. If you have any doubts please ask.

3.3.3 You must also ensure that your personal e-mail use:

- does not take priority over your responsibilities as a councillor;
- is minimal;
- does not cause unwarranted expense or liability to be incurred by the council;
- does not have a negative impact on the council in any way; and;
- is lawful and complies with this policy.

3.3.4 The council has limited storage space on its servers. You should therefore not store e-mail on the council’s systems unless it is work related. After being read, personal e-mail should be either deleted or forwarded to a personal e-mail account and then deleted. You should note though that e-mail is backed up on a regular basis and deleting it from the live system will not necessarily result in it being deleted for good.

3.3.5 If you make personal use of our facilities for sending and receiving e-mail you will be treated as having agreed to abide by the conditions imposed for their use, and consented to the council monitoring your personal e-mail in accordance with this policy. If you do not agree or consent to this then you must not use the system to send or receive personal e-mail.

4. USE OF INTERNET, INTRANET AND OTHER COUNCIL NETWORKS

4.1 We trust you to use the Internet sensibly. When visiting a website, information identifying your PC/tablet may be logged, therefore any activity you engage in via the Internet may impact on the council or your role as a councillor.
4.2 We recognise that individuals may have to carry out some personal tasks, e.g. for internet banking or online shopping, and this is permitted subject to the same rules as are set out for personal e-mail use in item 3.3 of this policy. However, any personal use is entirely at your own risk.

The council accepts no responsibility for any losses you may suffer.

4.3 You **must not** use your council e-mail address when using public websites for non-business purposes, such as online shopping, booking holidays etc.

4.4 Access to certain websites is blocked. If you have a particular need to access such sites, please contact the ICT help desk. Access will only be permitted for council purposes.

4.5 You must not:

- seek to gain access to restricted areas of the council’s network;
- access or try to access data which you know or ought to know is confidential;
- introduce any unauthorised software to the council’s systems. In particular you should not open any attachments with an .exe extension or open any attachments which appear to be programs, or download any browser “plug-ins” or programs except under the guidance of ICT Services.
- introduce any form of spyware, computer virus or similar malware.
- carry out any hacking activities
- use personal e-mail accounts (hotmail, googlemail etc.) on council equipment when connected to the corporate network (this does not prevent you using personal e-mail addresses as an identifier when using external websites).

You must:

- Inform the ICT Helpdesk immediately if you suspect your mobile device or members’ room computer may be infected with a virus or you have received an email which is malicious in any way, i.e. virus, spyware, fraudulent, etc. This will allow the extent of any damage to be limited.
- Inform ICT if you suspect that you have, or may have, unintentionally accessed a website which may breach the council’s policy.

5. **USE OF TELEPHONES, MOBILE PHONES AND TABLETS**

5.1 If you have been supplied with a mobile phone, or use telephones in the members’ room these should only be used to make calls on council business. You may be charged for the cost of private calls, particularly if the data package provided by the council, on mobile phones, is exceeded.

5.2 If the mobile telephone provided by the council also allows access to the internet and the corporate e-mail system, the requirements of this policy still apply. Misuse of council mobile devices may lead to disciplinary action and will be dealt with under the appropriate disciplinary procedure.

5.3 A separate policy relating to the use of tablet devices is shown at Appendix A.

6. **MISUSE OF THE COUNCILS FACILITIES AND SYSTEMS**
6.1 Misuse of the council’s facilities and systems, including its telephone, email and Internet systems, in breach of this policy will be treated seriously.

In particular, viewing, accessing, transmitting, posting, downloading, uploading, storing or communicating any of the following materials in the following ways, may result in a breach of the code of conduct (this list is not exhaustive):

- material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;
- offensive, obscene, derogatory or criminal material or material which is liable to bring the reputation of the council and any of its staff or its councillors into disrepute;
- any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;
- any material which, by intent or otherwise, harasses the recipient;
- any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;
- any material which violates the privacy of others or unfairly criticises or misrepresents others;
- confidential information about the council and any of its staff or councillors;
- any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the council);
- material in breach of copyright and/or other intellectual property rights;
- material which appears to be designed to affect support for a particular political party or candidate for election;
- online gambling; or
- chain letters or other junk mail of any kind.

7. WORKING REMOTELY

Working remotely is largely covered in the Tablet Acceptable Use policy at Appendix A. However the use of other mobile computer equipment e.g. smartphones, if supplied and also the use of your own computer equipment or other computer equipment whenever you are working on council business away from our offices is covered by this policy.

8. SOCIAL MEDIA POLICY

The council has a separate Social Media Policy which ensures that appropriate control mechanisms exist to minimise the risks to the council’s IT and communication systems, protect the council and its reputation and clarify to councillors and staff the appropriate use of social media.

This policy will be included in the Information Security Framework.

9. MONITORING OF COMMUNICATIONS BY THE COUNCIL

9.1 The council is ultimately responsible for all business communications but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. The council may monitor your business and personal communications for reasons which include:

- providing evidence of business transactions;
• ensuring that the council’s business procedures, policies and contracts are adhered to;
• complying with any legal obligations;
• monitoring standards of service;
• preventing or detecting unauthorised use of the council’s communications systems or criminal activities; and
• maintaining the effective operation of the council’s communications systems.

9.2 The council will monitor telephone, email and internet traffic data (i.e. sender, receiver, subject; non-business attachments to email, numbers called, the time and duration of calls; domain names of websites visited, the time and duration of visits, and files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes specified in this policy. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. By carrying out such activities using the council’s facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

9.3 All incoming email is scanned by McAfee on behalf of the Council, using virus-checking software.

The software will also block unsolicited marketing email (spam) and e-mail which have potentially inappropriate attachments. If there is a suspected virus in an e-mail which has been sent to you, the sender will automatically be notified and you will receive notice that the e-mail is not going to be delivered to you because it may contain a virus.

10. DATA PROTECTION AND FREEDOM OF INFORMATION

10.1 As a member of the council who uses our communications facilities, you will inevitably be involved in processing personal data as part of your role. Data protection is about the privacy of individuals, and is governed by the Data Protection Act 1998. This Act defines, among others, terms as follows:

"data" generally means information which is computerised or in a structured hard copy form;
"personal data" is data which can identify someone, such as a name, a job title, a photograph;
"processing" is anything you do with data – just having data amounts to processing; and
"data controller" is the person who controls the purposes and manner of processing of personal data –councillors, are each registered individually with the Information Commissioner as data controllers.

10.2 Whenever and wherever you are processing personal data you must keep it secret, confidential and secure, and you must take particular care not to disclose them to any other person (whether inside or outside the council) unless authorised to do so.

10.3 The Data Protection Act gives every individual the right to see all the information which any data controller holds about them. The Freedom of Information Act gives general rights to access most other information which the Council holds. It is another reason why personal remarks and opinions must be made or given responsibly, and they must be relevant and appropriate as well as accurate and justified.

10.4 To help you understand and comply with the council’s obligations Data Protection and Freedom of Information Acts you may be offered, and you may also request, training. Whenever you are unsure of what is required or you otherwise need guidance in data
protection, you should consult our Information Manager. Information about our data protection policies can be found on the loop.

11. **SYSTEM SECURITY**

The council has an Information Security Framework with which you should be familiar.
Appendix A

Chorley Council Tablet Acceptable Usage Policy for Councillors

Foreword

Use of tablet devices and new technology will enable council members to access information on the move, take advantage of secure Wi-Fi access in the main council buildings and contribute to the reduction in paper and printing costs outlined in the council’s digital strategy plans.

Mobile and home working takes information and equipment outside of the normal security arrangements that apply within and around council buildings.

This document is closely linked to the corporate Information Security Framework which details how both councillors and employees must work to ensure that we maintain the security of our information assets.

This policy only applies to elected members who will be asked to sign acceptance of its principles on receipt of a tablet.

Following receipt of tablets, councillors will no longer receive paper agenda or reports for meetings or council committees through the post.

These documents will be accessed through the modern.gov apps on the tablet.

These apps will enable you to read documents and make notes on screen in the same way you would with a paper copy.

Tablets can connect to the internet via Wi-Fi and if Wi-Fi is not available the device is capable of connecting to the internet via a 4G mobile telephone signal.

Your commitment:

- You must accept the requirements contained in the e-mail, internet, tablet and telephone acceptable use policy
- You must not delete any of the tablet software installed by the council. This software is essential to keep the device secure.
- You must not try to modify the tablet and you will not be able to install any other applications on the tablet.
- The device will be set up with a password before it is given to you. You must not disable this password or disclose it or any other passwords or usernames to anyone else.
- You must bring the tablet to meetings in a charged and useable condition.
- You must take care of the tablet and ensure it is safe and secure at all times to ensure the risk of theft is minimised.
- You must keep the tablets in the protective case supplied, to minimise the possibility of damage.
- If the tablet is lost, stolen or damaged you must immediately report it to ICT Services so that we can ensure the device is disabled and the data remotely removed. The device can be tracked by ICT Services. You may be charged for replacement.
- If the charger is lost or damaged you must immediately report it to ICT Services. You may be charged for replacement.
• You must return the tablet to ICT Services if you cease to be a council member.
• You must not allow anyone else to use the tablet.
• You must not access, view or download any illegal or inappropriate material. In particular, you should not access, view or download any material that would constitute a breach of the Council’s Information Security Framework.
• The council has installed software to try to prevent access to inappropriate web pages. This includes pornography and illegal sites as well as gambling and racist sites.

You must not:

• engage in activities on the internet which might bring the council into disrepute
• conduct yourself in a way that is detrimental to the council.
• use the internet in any way to send or post abusive, offensive, hateful or defamatory messages, especially those which concern members of the public, other councillors, employees or the council.
• post derogatory or offensive comments on the Internet
• act in a way which could damage the council’s reputation
• act in a way that damages the council’s or the public’s trust and confidence in a councillor’s fitness to undertake their role.
• post information that could constitute a breach of copyright or data protection legislation
• use your @chorley.gov.uk email addresses for personal business including purchasing items, booking holidays, banking etc.
• access any personal email account on your tablet
• allow interaction on websites that could cause damage to working relationships between councillors, employees and the public
• re-direct business e-mails to personal e-mail accounts
• stream unless on wifi as this uses excessive data. A 1GB per month data package is provided for business use.

Our commitment:

• We will configure the tablet so that you have all the necessary software and apps to enable paperless working for committee meetings.
• We will configure the tablet so that you can access your council e-mail account
• 3G or higher mobile ultra-broadband internet access will be provided.
• A capped data package of 1GB per month will be available on your tablet and unlimited wireless connection.
• We will provide you with initial training and ongoing support to get the most out of your tablet.
• Additional chargers will be made available for use in the Town Hall.
• We will install appropriate security software on your tablet to ensure that the data remains secure, provided that you comply with your commitments.
• We will continue to evaluate business apps that may be of use to you in your role as an elected member and will recommend these as appropriate
• You must not access, view or download any illegal or inappropriate material. In particular, you should not access, view or download any material that would constitute a breach of the Council’s Information Security Framework.
• The council has installed software to try to prevent access to inappropriate web pages. This includes pornography and illegal sites as well as gambling and racist sites.
I have received a copy of the following Chorley Council documents

- Councillors e-mail, internet, tablet and telephone acceptable use policy
- Tablet Acceptable Usage Policy Appendix A

I understand that the council’s Information and Communications Technology (ICT) systems and associated equipment are to be used for conducting council business or for personal use only as stated in the policy documents.

I have read the policy documents and agree to abide by all the terms and conditions set out in the documents for the duration of my employment or association with the council.

I am aware that the council may, where it considers it to have reasonable grounds to do so, and without notice to me, monitor or examine all or any telephone, e-mail or internet traffic and documents or files initiated, manipulated, stored, responded to or examined by me.

I am aware that violations of the policies may amount to a breach of the Code of Conduct. I understand that I may be personally liable for any criminal offence, which I may commit in relation to these policies.

I further understand that my internet usage and telephone and e-mail communications must at all times reflect the good name and character of Chorley Council.

I understand that the policies and this document may be amended at any time and that I will be informed of changes in the manner described in the policy.

I accept that I am responsible for ensuring my personal knowledge and understanding of any change to the policy.

Signature .................................................. Date ..............................................

Printed name ........................................................................................................