Chorley Council

Email, Internet and Telephone Acceptable Usage Policy – for Councillors

Beacon Authority 2005-2009 Transforming Services: Citizen Engagement and Empowerment

Beacon Authority 2009-2010 Cohesive and resilient communities

Beacon Authority 2009-2010 Better outcomes for people and places

Document Control

Organisation	Chorley Council
Title	Email, Internet & Telephone Acceptable Usage Policy
Author	Andrew Docherty/Tim Murphy
Filename	AUP.doc
Owner	Corporate Director (Human Resources & Organisational Development)
Subject	Information Security
Protective Marking	Unclassified
Review date	19th[st] November 2010

Revision History

Revision Date	Reviser	Previous Version	Description of Revision
	Corporate Directors Governance & (ICT)	N/A	Version submitted to Cabinet

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Executive Cabinet		

Document Distribution

This document will be distributed to Members via the Council's intranet.

Contents

Foreword

This is an important policy. It aims 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 Members and employees of the Council, 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. This policy only applies to elected Members. A similar policy which recognises the different positions of staff and Members applies to the Council's staff.

This policy and that for staff:

- Set out general rules for the acceptable use of the system
- Point out that the way we use the facilities made available to us reflects on the Council and can commit the Council legally
- Remind 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 IT services before sending confidential or sensitive information via email
- Describes how and when personal use of e-mail, Internet and telephones is permissible
- Requires us to remove personal e-mail from the Council's systems
- Prohibits private use of Council provided mobile phones (where the facility to have a private Line 2 is available)
- Prohibits the use of Council e-mail addresses on public websites for non business purposes

The policy also sets out the circumstances in which the Council may monitor our communications.

There can be serious consequences for failing to follow this policy but we do not want to catch anyone out. If you need any clarification of anything in this policy please ask your Group Leader and/or the Monitoring Officer.

Donna Hall
Chief Executive

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. Please read it carefully.

1.2. WHO DOES THIS POLICY APPLY TO?

This Policy applies all Members, using the Council's ICT equipment or systems.

1.3. WHAT FACILITIES DOES THIS POLICY COVER?

The facilities covered by this document includes access to all communication facilities provided by the Council including Internet and e-mail services, telephones, fax machines, 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 could result in a complaint to the Standards Committee and/or in the withdrawal of permission to use the Council's equipment for personal purposes. Less serious breaches may result in formal or informal action being taken dependent upon the nature of the breach.

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 discuss it with your Group Leader or the Monitoring Officer.

IMPORTANT

Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes. The most up to date copy of the policy will be published on theloop.

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 other Members 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 email. 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. Any user who is unclear about the appropriateness of any material should consult their line manager before sending it.

3. USE OF ELECTRONIC MAIL

3.1. GENERALLY

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

This e-mail and any attached files are confidential and may also be legally privileged. They are intended solely for the intended addressee. If they have come to you in error you must not use, copy or communicate them to anyone. Please advise the sender and permanently delete the e-mail and attachments.

Please note that while Chorley Council has policies in place requiring its staff to use e-mail in an appropriate manner, any views expressed in this message are those of the individual sender and may not necessarily reflect the views of Chorley Council.

Chorley Council may monitor e-mails sent or received.

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 email folders nor send any email purporting to come from another person.

3.1.3. 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 IT Services and ask for the email to be encrypted. It is, in any event, good practice to re-read and check an email before sending and to confirm that you are sending the e-mail to the right person.

3.1.4. If you copy an email to others, it may breach the Data Protection Act if it reveals all the recipients' email 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.

3.1.5. 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 email to more than one recipient. If in doubt, seek advice from the Monitoring Officer .

3.2. BUSINESS USE

3.2.1. If the email message or attachment contains information which is time-critical, bear in mind that an email 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 email has been received and read.

3.2.3. In light of the security risks inherent in some web-based email accounts, you must not email 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 email 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 our 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 Members 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 doubt contact your Group Leader and/or the Monitoring Officer.

3.3.3. You must also ensure that your personal email 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 email should be either deleted or forwarded to a personal email account and then deleted. You should note

though that email 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 email you will be treated as having agreed to abide by the conditions imposed for their use, and consented to the Council monitoring your personal email 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. Bear in mind at all times that when visiting a website, information identifying your PC may be logged. Therefore any activity you engage in via the Internet may affect the Council.

4.2. We recognise that individuals may have to carry out some personal tasks during working hours, e.g. for Internet banking or online shopping, and this is permitted subject to the same rules as are set out for personal email 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 email address when using public websites for non-business purposes, such as online shopping. Doing so results in you and the Council receiving substantial amounts of unwanted email.

4.4. Access to certain websites is blocked. If you have a particular business need to access such sites, please contact the IT help desk. Access will only be permitted for work 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 IT Services.
- intentionally or recklessly 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 (this does not prevent you using personal e-mail addresses as an identifier when using external websites).

4.6. You must:

- Inform the ICT Helpdesk immediately if you suspect your 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 AND MOBILE PHONES

5.1. Where the Council provides a separate home phone line for members this should only be used to make calls on Council business. These requirements also apply if the Council makes a mobile phone available.

5.2. The Council's mobile phone arrangements allow for a Line 2 to be available. Calls made on Line 2 are charged directly to the individual whereas the cost of calls on Line 1 is borne by the Council. Consequently no personal calls should be made on Line 1.

5.3. If the mobile telephone provided by the Council also allows access to the Internet and the corporate email system, the requirements of this policy still apply. In addition, members of staff using these phones should ensure they are familiar with the Mobile Computing and Teleworking Policy that forms part of the Information Security Framework and ensure compliance with it.

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 and may result in a referral to the Standards Committee. In particular, viewing, accessing, transmitting, posting, downloading, uploading, storing or communicating any of the following materials in the following ways, will amount to gross misconduct capable of resulting in summary dismissal (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 Members 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 Members ;
- 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

The Council has a Mobile Computing and Teleworking Policy which applies to your use of our laptops and other mobile computer equipment (including smartphones and PDA's), and also to your use of your own computer equipment or other computer equipment whenever you are working on Council business away from our offices (working remotely). If you work remotely or take equipment off the Council's premises you must ensure that you are familiar with that policy.

8. MINI WEBSITES AND OTHER MATTERS

8.1. Every member of the Council is entitled to be provided with a mini website. Members who take up this opportunity will be provided with separate guidance on appropriate content. However, this policy applies equally to mini websites as it does to other facilities provided by the Council.

8.2. You must not set up an account or group or publish anything on a social networking site or any other website on behalf of the Council or in the name of the Council or any of its services. Only the Council's communications team have authorisation to do this.

8.3. Some Members may choose to publish content on the Internet without using Council facilities. This policy will not generally apply to privately published material. However. Members should be aware that the Code of Conduct applies whenever they are conducting or giving the impression that they are conducting the business of the Authority.

•

8. 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 with staff 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 Messagelabs on behalf of the Council, using virus-checking software. The software will also block unsolicited marketing email (spam) and email which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to you, the sender will automatically be notified and you will receive notice that the email 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. If in doubt get help from the Monitoring Officer or the Information Manager.

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 theloop.

.

11. SYSTEM SECURITY

The Council has an Information Security Framework which you should also ensure that you are familiar with.

Authorised User Agreement

I have received a copy of the following Chorley Council documents

- **Internet, e-mail and telephone acceptable use policy**
- **Information Security Framework.**

I understand that the Councils 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 and could result in a complaint to the Standards Committee. 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 ……..