Borough Telford & Wrekin

E-mail and Internet Usage

Code of Practice

clicking on this symbol in the left margin will return you to the contents page.

Contacts

ICT Service Desk	84444		Data Protection Officer	82530
Internal Audit IT Contact	83117		Legal Services	83245

Introduction

The Council recognises that both e-mail and the Internet are of increasing importance to the work carried out by Officers and Members. Many of our citizens, partners and suppliers have an expectation that they can deal with us through these mediums. There is pressure from central government to adopt these technologies and take advantage of the opportunities they offer. E-Mail, the Internet and the Intranet are key components in implementing the Council's communications strategy both internally and externally.

Because of the open nature and ready availability of e-mail and Internet services, there are potential dangers to the Council. These could arise from malicious intent, carelessness or from complacency. All of the risks associated with normal written or verbal communication apply to electronic communication as well. There are additional areas of concern that relate specifically to electronic transfer of information.

This document is to be used as a guideline for use of e-mail and Internet by Officers and Members. It defines minimum acceptable use standards, and is designed to protect the Council, its employees and the elected members from accusations of misuse or malpractice.

Signing this document is a prerequisite for any Officer or Member who may as part of their role with the Council access the Internet or use e-mail. This is regardless of whether the access is through fixed or portable equipment, and whether the equipment is owned, supplied or approved by the council. Even if the council does not own the equipment used, it is essential that standards relating to accessing appropriate content and maintaining the good reputation of the council be observed.

It should be noted that references to 'e-mail' within this document apply to both internal and external use of the medium. Unless specifically excluded, references to the Internet should also be taken to include the Intranet, Electronic Bulletin Boards, Online discussion forums and similar electronic information exchanges.

The principles outlined in this document should always be read and applied alongside other rules, regulations or guidelines issued from time to time by the Council. In particular, nothing in this document limits or replaces the Council's Standing Orders, Financial Regulations or Security Policy.

In the event of actual or suspected misuse of e-mail or the Internet, authorisation may be withdrawn from an individual or group of users by a member of the Corporate Board, the appropriate Head of Service, Head of ICT, the Audit Services Manager or the relevant political group leader. Details will be reported to the relevant manager and to Internal Audit. In addition, action may be taken against an employee through the disciplinary process, or in the case of a member by reference to the Standards Committee.

It is not intended that this document provide instruction or training in the use of e-mail or the Internet.

Security Principles

It is essential that this document be used in conjunction with the Council's Security Policy, which defines rules for the protection of information and the technology used to store and retrieve it. It also identifies relevant legislation.

Full copies of the Security Policy are in the Managers Handbook. A summary of the Security Policy is available to all employees.

Key principles from the Policy relevant to e-mail and Internet usage are shown below:

➢ Any violation of the rules and procedures should be reported.

➢ Deliberate or serious violation of the rules and procedures will result in disciplinary action.

➢ It is your duty to be aware of your legal responsibilities and to comply with relevant legislation.

➢ Appropriate levels of security and authorisation control access to computer systems.

➢ Physical security of equipment, including not leaving a "logged on" system unattended is equally important.

➢ Maintain regular backups of information.

➢ Do not download or install unauthorised software onto Council owned equipment.

➢ Always follow the Council's anti-virus strategy.

➢ Before exchanging information electronically, always verify that the recipient is who they say, and is authorised to receive that information.

➢ Do not disclose information regarding security or access to unauthorised people.

Additional safeguards apply to portable equipment, or equipment not permanently based within council premises.

➢ Wherever possible, password protection should be used to disable ready access to the system.
➢ Precautions must be taken to ensure that unauthorised users cannot gain access to the equipment.
➢ The authorised user of the equipment will be responsible for any use, in particular access to the Internet, or e-mails sent on their behalf.
➢ Never leave equipment unattended in a car or public place.

Legal Implications

The list below identifies the key areas of legislation that may apply to the use of e-mail and the Internet. It is not exclusive, and if there is any doubt seek advice about specific legislation from Legal or from Internal Audit.

- ➢ Employment Conditions

- ➢ Copyright & Intellectual Property Rights

- ➢ Defamation & Libel

- ➢ Human Rights Act

- ➢ Freedom of Information

- ➢ Regulation of Investigatory Powers

- ➢ Data Protection

- ➢ Computer Misuse

- ➢ Contract Law

- ➢ Pornography and Obscene Publications

- ➢ EU Directives

- ➢ Public Sector Legislation

- ➢ Service Specific Legislation

- ➢ Equalities Legislation

- ➢ Professional Body Guidelines and Codes of Conduct

E-mail Guidelines

E-mail is an efficient and effective way of communicating both internally and externally. A strategic decision has been taken that no differentiation be made between the ability to send messages within Telford & Wrekin Council and the option of sending messages to other organisations. The following guidelines are designed to ensure that the maximum benefit is obtained, while protecting the organisation and individuals from accidental or malicious misuse.

- *The Council monitors use, and filters content of e-mail, both sent and received.*
- *E-mails captured in the filtering software that are considered to be non-business related and offensive will be deleted without forwarding.*
- *Abuse or misuse of the service will be reported to your manager and Internal Audit and may lead to disciplinary action. Defamatory or libellous comments in an e-mail may render the sender personally liable to civil action.*

DO:

Consider whether e-mail is the best way to send a message:
- messages may not be secure unless encryption is employed.
- messages may not be read immediately.
- messages may be produced as proof that you said something.
- messages may be held to be legally binding.
- messages may be subject to tampering after delivery or sending.
- messages may continue to exist after you think you have deleted them.

Apply the same principles you would use with a printed memo:
- Content should be clear and not open to misinterpretation.
- Include a meaningful subject line.
- Include your position and contact details the first time you contact someone.
- Use standard fonts and effects to ensure legibility on other systems.
- Only copy to those who need to receive a copy.

Check incoming mail regularly and respond promptly.
- The Council has guidelines for responding to external contacts by phone or mail.

Ensure the recipient can open attachments if you use them.

Make use of the "out-of-office" facilities when you are away for any period.

Forward messages about Viruses DIRECTLY and ONLY to the Helpdesk.

DON'T:

Use e-mail to avoid difficult face-to-face communication.
Use e-mail to send confidential information without appropriate encryption.
Use e-mail to send personal information without authorisation.
Send messages that may be read as obscene, harassing, intimidating or discriminatory.
Send messages in anger, even in response to abusive mail.
Send messages in CAPITALS - it may be interpreted as shouting.
Send messages to "everyone" without authorisation from a senior manager.
Send simple messages as complicated attachments.
Open attachments that you are not expecting or from unknown sources.
Forward or respond to junk mail, chain letters, virus hoaxes etc.

Internet Guidelines

Much valuable information is available from the Internet, particularly the part known as the World Wide Web (WWW). Many organisations use the Web to advertise their products or services, often in preference to other means of advertising. Central Government also uses the medium to publish guidance and details of legislation.

The Web also contains much that is unpleasant, inaccurate, unnecessary or illegal. For this reason it is important that staff and elected members understand and abide by the guidelines below.

- *When using council equipment, do not link to the Internet other than through an official connection sanctioned by the Central IM&T Service.*
- *Internet Access is personal to your userid; you will be held responsible for any use or misuse traced to your userid.*
- *Remember that use of the Internet and sites visited is monitored and filtered by the Council. Abuse or misuse of the service will be reported to your manager and Internal Audit and may lead to disciplinary action.*

Only visit sites necessary for you to carry out your job.
- ➤ If you regularly use a site, save a bookmark in your Favourites folder.
- ➤ Remain focussed - it is easy to be sidetracked by "interesting" links.
- ➤ Only print information necessary for your work.
- ➤ If you are presented with an unsuitable site, report it to the Helpdesk.

Check the accuracy and currency of information retrieved before relying on it.
- ➤ Remember that not everything is available or accessible on the Web.

Do not download or install software from the Internet unless you have specific authorisation.
- ➤ Downloaded software is a major source of virus infection.
- ➤ Licensing and copyright relating to downloaded software can be complex.
- ➤ Untested software can cause costly interruptions to your own or other peoples work.

Remember that copyright laws apply to information found on the Internet,.
- ➤ Do not use downloaded materials as your own.
- ➤ Do not assume that images or other materials are freely available for use.

If you use newsgroups or mailing lists be sensitive to the Councils interests.
- ➤ Only offer advice or information that is appropriate to your role.
- ➤ Do not offer opinions contrary to the Council's interests.
- ➤ Do not take part in political discussions unless it is part of your role.

Unless specifically authorised, do not use the Internet to enter into financial or contractual agreements on behalf of the Council. Do not subscribe to services on-line without authorisation.

Always remain aware of the legal implications of using the Internet.
- ➤ Do not visit sites or download files containing obscene, pornographic, discriminatory or otherwise offensive materials.
- ➤ Do not infringe copyright or licensing arrangements.
- ➤ Do not attempt to circumvent security systems, or in any other way attempt to access systems or information for which you are not authorised.

Virtual Private Network (VPN)

In cases where a direct link to the Council's main network is not feasible, an indirect link may be provided through the Internet. To ensure that this is secure, a Virtual Private Network (VPN) is established which authenticates the user, and encrypts any information sent across the public network. An example is the service offered through the PCs and laptops supplied to Members.

Authentication is achieved by combining a userid with a pass code generated by an "Active Card". This code is changed every couple of minutes. The card has been synchronised with a server at the Council, which knows what code will be generated at any particular time. This makes it impossible for someone without the Active Card to guess the pass code.

VPN access may also be provided as a service from a non-Council owned piece of equipment, subject to the points made below.

> ➢ The user will have signed the relevant parts of this document.
> ➢ The equipment & software used meets minimum specifications defined by the council.
> ➢ A virus scanner will suitably protect the equipment.
> ➢ The council cannot accept responsibility for the maintenance and repair of the equipment.
> ➢ The council cannot guarantee speed of connection, nor that any particular piece of non-council supplied equipment will work with this system.

Personal Use

The e-mail and Internet services are installed expressly for the purpose of supporting the Council's business.

The Council is prepared to allow limited personal use of the services to employees and members subject to the conditions outlined below.

All use of the Internet or e-mail using Council equipment or a Council Connection is subject to monitoring and filtering by the Council. This includes sites visited and content of e-mails.

➢ Authorisation to use the service can be revoked or limited at any time by the Head of IM&T or nominee if it is considered to be prejudicing the delivery of the Councils own services.

➢ Authorisation to use the service by any individual can be revoked or limited by their Head of Service, Business Manager or nominee at any time if it is considered to be adversely affecting the delivery of some part of the Council's service either directly or indirectly. A similar condition will apply to members, with political group leaders being the arbiters.

➢ All guidelines for behaviour outlined in the rest of this document will apply to any use of e-mail or the Internet through the Councils connection or through equipment supplied and owned by the Council.

➢ Such access should only be undertaken in the persons own time, not when they should be doing their normal work. Unless otherwise agreed by the relevant line manager, this is assumed to be outside of the core time defined in the Councils' Flexitime system.

➢ Under no circumstances should the service be used to operate or support a business or equivalent private venture.

➢ Under no circumstances should the service be used for any purpose that may be considered illegal or mischievous.

➢ Printing the results of private use of the service will be subject to the same charges levied for personal use of photocopiers. Staff are responsible for ensuring that they record and pay for any personal printing on Council equipment.

➢ Use of the service in such a way as to threaten the normal operation of the Council's business, or to damage the reputation of the Council, will be reported to your manager and internal audit. Sanctions will range from temporary or permanent withdrawal of access, to disciplinary action under the Council's disciplinary scheme. In the case of members, the action may include reference to the Standards Committee.

➢ Where access is not through the Council's permanent connection, the cost of using the Internet or e-mail for personal purposes will be the responsibility of the individual.

➢ No guarantee of availability or quality of service is made.
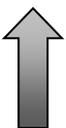
Registering for Internet and / or e-mail Use

For control and monitoring purposes, it is essential that individual users of the services can be identified.

Access to the Internet will only be available when the PC is logged on with the ID of a person who has signed and returned a "Request for Authorisation of Internet Access". Each user of the Internet will need to have signed a copy of the form and had their ID authorised. When a PC is accessing the Internet, the person associated with the ID logged on will be responsible for all Internet use during that session.

A new e-mail account will only be made available when the user has signed and returned a "Request for Authorisation to use E-mail". For existing accounts, access will be suspended if a form is not returned within a month of this document being circulated.

Monitoring of Use

The e-mail and Internet services are installed expressly for the purpose of supporting the Council's business. To maintain the quality, security and integrity of the service the Council uses various monitoring, filtering and capture tools. Objectives of this include:
- Detection of Viruses
- Prevention of unauthorised access to Council systems
- Measuring bandwidth usage, including number & size of e-mails sent/received
- Identifying Internet Sites visited and Sites blocked from access
- Monitoring times when access is made and when messages are sent
- Identifying e-mail origins & destinations
- Identifying e-mail content, i.e. use of inappropriate language
- Identifying e-mail content, i.e. types of attachments

Users should be aware that it is not possible to differentiate between business and personal use. All usage is subject to monitoring. All e-mail is filtered for content. E-mails captured in the filtering software that are considered non-business related and offensive will be deleted without forwarding.

The Council reserves to right to monitor and read any e-mail sent or received, together with any attached files, including accessing historical e-mail records.
By signing the AUP, you are deemed to have given your consent.

Actions
- Abuse or misuse of e-mail or the internet will be reported to managers, and copied to internal audit
- Further action may be taken through the Council's disciplinary procedure, or in the case of elected members through the Standards Committee.
- In extreme cases, the Council may choose to involve the police or other external agencies.

Costs

E-mail and Internet are corporate services currently funded by means of a recharge to Service Areas based on number of e-mail accounts and number of authorised Internet users. A recharge code will need to be supplied for both e-mail and internet services.

Charges are based on the cost of delivering, maintaining and developing the services and will be reviewed on an annual basis.

Request for Authorisation to Use E-mail (effective from April 2003)

Please complete all Greyed out areas. Return this form to:

ICT Contact Centre
Civic Offices
PO Box 215
Telford
TF3 4LF

Administration only:
ICT Contact Centre Call Ref:

Note that, for new users, the name you give will become your external e-mail address, so it should be how people know you:
e.g. james.jones@telford.gov.uk or jim.jones@telford.gov.uk

Renewal or First Access.			
Name.		Logon I.D.	
Portfolio / Political Group.			
Service Area / Business Unit.			
Primary Work base. (or mobile)			
Telephone no.			
PC ID you will use. (or details of other means of access)			

I have read and understood, and agree to abide by the "Borough of Telford & Wrekin e-mail & Internet Code of Practice".

I understand that the Council will monitor and filter any use I make of the service, including checking the content of e-mail messages and attachments.
By signing this document I understand that I am consenting to this.

I understand that I am authorised to use the service to support my official role in the Council and for personal use within the restrictions laid down in the Code of Practice.

I understand that any personal use of the service must be carried out in my own time, and is subject to the same restrictions and guidelines as my official usage.

Signed										
Print Name										
Date										
Job Title										
Cost Code			**5**	**5**	**0**					
Bus. Manager / Budget Holder										
For ICT Contact Centre Use Only										
Date Received										
Date Actioned										
Customer Notified										

Request for Authorisation of Internet Access (effective from April 2003)

Please complete all grey areas and return this form to:

ICT Contact Centre
Civic Offices
PO Box 215
Telford
TF3 4LF

Administration only:
ICT Contact Centre Call Ref:

Renewal or First Access.			
Name.		Logon I.D.	
Portfolio / Political Group.			
Service Area / Business Unit.			
Primary Work base. (or mobile)			
Telephone no.			
PC ID you will use? (Or details of other means of access.)			

I have read and understood, and agree to abide by the "Borough of Telford & Wrekin e-mail & Internet Code of Practice".

I understand that the Council will monitor and filter any use I make of the service. By signing this document, I understand that I am consenting to this.

I understand that I am authorised to use the service to support my official role in the Council and for personal use within the restrictions laid down in the Code of Practice.

I understand that any personal use of the service must be carried out in my own time, and is subject to the same restrictions and guidelines as my official usage.

Signed	
Print Name	
Date	
Job Title	

Head of Service / Business Manager Authorisation

I agree that the person identified in this form requires access to the Internet to carry out their role. I have identified the cost code for recharge of the cost.

Cost Code			**5**	**5**	**0**					
Signed										
Print Name										
Date										
Job Title										

For IM&T Use Only	
Date Received	
Date Actioned	
Customer Notified	