Wyre Borough Council Computer Use Policy

Wyre Borough Council Computer Use Policy

Introduction

This policy covers the use by employees and elected members of any IT equipment provided by the council.

The policy governs use of e-mail accounts and addresses and Internet service provider (ISP) facilities provided through the council as well as other mobile devices such as the use of council laptops. It also governs the connection of any electronic device to the Council’s I.T. network.

In the rest of this policy, “facilities” means anything covered in the preceding paragraph and “user” means any employee or elected member using any of the facilities. “Mobile device” includes notebooks, laptops, Memory Sticks/Pen Drives, Personal Data Assistants (PDA’s) or any other mobile device. “Viruses” means virus, Trojan, worm, malware, japeware, adware and any malicious software.

Every user has a responsibility to maintain and enhance the Council's public image and to use the facilities in an appropriate manner. This policy has been established to inform users of what is and is not appropriate. Any improper use of the facilities is not acceptable and may be dealt with through the Council's disciplinary process or through the members’ code of conduct.

Access

Access to the Internet and e-mail must normally be through the use of the corporate Internet/e-mail system via the corporate network. Individuals using the network must not use modems or any other communication link attached to their PC's to access the Internet or any other service without the written permission of the IT Systems / Software Manager.

All users allowed access to the Internet/e-mail systems will be required to sign a declaration that they have read and understood this Policy and are prepared to abide by it.

The installation and configuration of software, for the purpose of Internet access or the collection and delivery of e-mail, must be undertaken by a member of the IT team and must not be changed without the authority of the IT Systems / Software Manager.

Access to the Council’s information systems via the facilities is subject to password security. Users must not reveal their security password to any other person and passwords must not be recorded (e.g. written down) in any form. The IT Helpdesk can assist in resetting forgotten passwords.

Users must ‘lockdown’ their facilities when not in use or when away from their desk.

Only authorised users can use the facilities and third party access by any individual who has not signed up to the Computer Use Policy is prohibited.

Communications

Each user is responsible for the content of all data, text, audio or images that they place or send via or using the facilities. All messages must contain the user's full name as a users email address is not a valid name. No e-mail or other electronic communication will be sent which hides the identity of the sender or represents the sender as someone else or someone from another organisation.

For efficiency purposes distribution lists should be limited and mass emailing or spamming (i.e. emailing to a large audience) is discouraged.

Users are recommended to utilise the signature facility when sending emails. Any messages or information sent by a user to another individual outside of the council via an electronic network (e.g. bulletin board, online service or Internet) are statements that reflect on the Council. The IT team will ensure that all external e-mail has the Council’s standard disclaimer automatically attached to the end of the message (appendix A). Non-standard disclaimers must not be used.

Acceptable Uses of the Internet, E-mail and Data

All Users will use the Internet and email for-

- Business communication on behalf of the council;
- Lawful research into matters connected with their duties; this includes ward business and matters in connection with any special responsibility such as chairmanship.
- Political purposes so long as they are connected with the council; For example, use in connection with the leadership or other role in a political group in the council would be appropriate; as would use in connection with work as a Parish Councillor or use in connection with an outside body for which you are a Council nominee. Use in connection with any other outside position or office in a political party or other organisation would not be appropriate and would be considered a potential breach of the councillors’ code of conduct.
- Personal purposes which do not interfere with work productivity, do not take up excessive amounts of time, are not connected with any private business enterprise or other employment and do not result in the dissemination of any information held by the council that is not in the public domain.

The Council accepts no responsibility for private use of the facilities or any loss, costs or liability, which the user or any other person may suffer as a result of the private use of the facilities.

The facilities must not be used for viewing, transmitting, retrieving or storing any material of a discriminatory or harassing nature or material that is obscene or pornographic.

The transmitting, retrieving and storage of any communications containing personal data must comply with the Data Protection Act 1998. A summary of these requirements can be seen on the Council’s intranet.

No derogatory or inflammatory material about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted, retrieved or stored. Further information is available on the Equality and Diversity section of the intranet.

No abusive, profane or offensive language is to be transmitted, retrieved or stored.

The facilities must not be used for any other purposes, which are illegal, or against Council policy or contrary to the Council's legitimate interest.

All users will be able to access confidential Council material using the facilities. Every user is responsible for the continued security of any such confidential information, which they receive, including the security of any storage of such information. Users are advised of their obligations under the Code of Conduct not to disclose such confidential information to third parties. The relevant Codes of Conduct, both for employees and councillors, are available on the intranet.

For further guidance please see appendix B.

Training

Training is a requisite for all users of the Internet/e-mail systems. This will be provided in conjunction with the IT Section who can be contacted by e-mail at HDesk@wyrebc.gov.uk.

Software and Viruses

It is important that the Council's corporate networks are protected from viruses and that the following points are strictly adhered to:

Internet - there will be no unauthorised downloading of any software. All software downloaded must be registered to the Council. Users should contact the IT Team if they have any questions.

E-mail - all Wyre Borough Council IT gateway e-mails are scanned for known viruses. This should only be used as an indication and users should be cautious of opening attachments from un-trusted sources. The council's firewall is likely to intercept emails containing executable and certain other file types. You must not therefore arrange to be sent any such attachments via the facilities.

Only equipment authorised by the IT Team may be connected to the Council's I.T. network All PC's/laptops with Internet access must have access to a virus checker. Anti virus updates are automatically deployed when mobile devices are connected to the network. The IT Team may require access to all PC's and mobile media devices at any time to check for computer viruses. Any indication of a virus must be immediately reported to the IT Helpdesk.

Users shall not interfere with IT installed software packages, configurations or switches. The Council's firewall and anti virus measures must not be disabled.

Unless there is a valid business case for its use, the 'macro' feature in Microsoft Office applications should be disabled. Where 'macros' are used they should be digitally signed and be configured to run in HIGH security mode, to ensure that only macros from administrator-controlled sources i.e. trusted locations are run.

Any prompt, suggesting the automatic upgrading of software (such as Acrobat Reader), should be declined and the matter referred to the IT Helpdesk.

Connecting mobile media devices to the Council's network

The use of mobile media devices (such as notebooks, tablets, CDs, Floppy disks, Memory Sticks / Pen Drives, Cameras, Phones, Portable Media Devices e.g. iPods and Handheld Pocket PCs) presents additional risks to the Council's information systems including:-

- Increased susceptibility to viruses;
- Risk of unauthorised removal of sensitive / confidential data;
- Use of systems for non work related activities; and
- Reduction in productivity of staff (use of games, music, pictures).

All connections to the Council's I.T. network are monitored and will be screened to ensure that only authorised connections are permitted. Only where a business case is made for justifying such access will permission be granted.

Information that is removed from the networked systems owned by the Council must be treated with care. Caution must be used when copying data onto any mobile media device. This also applies to sending data attached to emails. Data removed from the network is at greater risk; it could be lost, intercepted, copied, etc. Measures must be taken to protect this data via encryption or the use of password access.

Mobile devises which connect to the Council's email facilities can be securely remote wiped if required. All users should be aware that in the event of a security incident IT may be required to initiate this function without prior warning. This would include the Users own personal device if this has been authorised for use.

Managers who authorise the use of mobile media devices should be aware of the associated risks and the possible consequences of their actions.

Copyright Issues

Users shall not knowingly infringe any copyrights by using, copying or dealing in any other way with copyrighted material without all necessary consents. It is the policy of Wyre Borough Council to respect all computer software copyrights and adhere to the Terms and Conditions of any licence to which Wyre Borough Council is a party. Wyre Borough Council will not condone the use of any software that does not have a licence and any employee found to be using, or in possession of, unlicensed software will be the subject of disciplinary procedures. Users should be aware that the Council is actively seeking the FAST (Federation Against Software Theft) accreditation.

Security and Monitoring

All incoming and outgoing emails are monitored for improper content. Such monitoring may be routine, random or targeted. Targeted monitoring will only be carried out where there are grounds to believe that a contravention of this policy has taken place. Any emails contravening these guidelines will be quarantined or deleted. The protocol for dealing with email can be seen on the IT Services section of the intranet.

The Council's Internet gateway is routinely monitored for cost control usage patterns and the accessing of improper material. The Council will investigate any apparent improper use. If any user feels that they have mistakenly accessed improper material, or are aware of or suspect another user who is not complying with the Computer Use policy, they must notify the IT Helpdesk immediately. The Council also reserves the right to implement filters and other means of blocking access to and from certain parts of the Internet from the Council's gateway.

All messages created, sent or retrieved over the Council's Internet/e-mail systems are the property of the Council and should be considered public information. The IT Section will limit the size of e-mails and attachments to ensure that network and system performance is not hindered.

The council may audit any mobile media device or PC at any time. Such audit may be carried out remotely and without specific notice or consent if the equipment is connected to the council's network. The council may take possession of equipment at any time in order to carry out an audit.

Users of the Government Connect Secure Extranet (GCSX) must also sign a Personal Commitment Statement confirming their responsibilities and acceptance that communications sent or received by that means may be intercepted, monitored and/or recorded for lawful purposes.

Return of equipment by all users

All equipment issued to users remains the property of the council. It must not be sold, given, or lent out to any third party. Mobile media devices must always be kept in a safe place and never left unattended in public. Proper precautions must be taken to keep them safe from theft or accidental damage and users must not deliberately damage or modify them in any way. The council will carry out any necessary repairs and maintenance.

Equipment must be returned immediately on termination of contract or when a member ceases to be a member of the council, or at any other time if demanded in writing on behalf of the council.

Policy Updates

Due to the changing nature of the facilities available through the Internet and e-mail, this document and any associated policies will be altered when necessary. In order to ensure that the latest copy is referred to, the official copy will be stored on the Councils Intranet Users will be notified of any amendments that have been made. It is the responsibility of the user to acquaint themselves with the amendments to this or any other policies that may change from time to time.

Violations

Any employee who misuses or abuses the facilities will be subject to the Council's disciplinary procedures. Abuse of the facility (e.g. gross or continued misuse) may potentially lead to the termination of employment. If necessary, the Council also reserves the right to advise appropriate bodies of any illegal violations.

Any elected member who misuses or abuses the privilege of the facilities may result in their withdrawal. Additionally, such breach may be dealt with, if appropriate, as a breach of the members' code of conduct.

Declaration

I have read and understood the Computer Use Policy above and agree to comply with the Policy.

Employee / Member Name

……………………………………..……………………………………………………………………………………..

Employee / Member Signature

………...……………..

Date ………………………………………………………………………………..……………………………

<u>Appendix A</u>

External E-mail Disclaimer

This e-mail contains information intended for the addressee only, may be confidential, and may be the subject of legal and/or professional privilege.

If you are not the intended recipient, any disclosure, copying, distribution or other action taken in reliance of the information contained in this e-mail is strictly prohibited.

Any views expressed by the sender of this message are not necessarily those of Wyre Borough Council.

If you have received this transmission in error, please use the reply function to tell us and then permanently delete what you have received.

Please note: Incoming and outgoing e-mail messages are routinely monitored for compliance with our policy on the use of electronic communications. Wyre Borough Council scans outgoing e-mails for viruses, and it is your responsibility to carry out any checks before opening the e-mail and/or attachments.

Appendix B

Acceptable Uses of the Internet, E-mail and Data – Further Guidance

The following guidance is non-exhaustive and is intended to help you in understanding good practice when using the facilities. If you are unsure or do require further assistance please contact the IT Help Desk.

- Use of facilities such as Apple iTunes or AmazonMP3 for music, movies, TV and applications is prohibited.
- The default media player (usually Windows Media Player) should not be used for playing, converting, duplicating or copying of any CD/DVD content either via mobile media devices or the computers internal hard drive.
- Examples of copyrighted material can include computer software, magazine articles, reports, photographs, music and video files.
- All software installations should be completed by the IT Team. PC and video games should not be installed on any Council equipment.
- A tablet device is typically a computer with touch screen capabilities such as an IPad, Playbook, Galaxy Tab, all of which must be authorised by the IT Team prior to being connected to the network.
- A secure remote wipe of a mobile device will remove all content, settings, applications and features on the device.
- The Councils I.T. Network includes both Local and Wide Area Network links.
- On-line gambling and accessing such websites is prohibited.
- Peer-to-peer (P2P) networks are commonly used to transmit music and video files across the internet. Unauthorised P2P file sharing is prohibited.
- The internet has now developed into an integral part of peoples' day-to-day lives through the introduction of on-line banking and shopping facilities and has, in many instances, replaced the necessity to physically visit the High Street / Retail Outlets. Care should be taken when accessing such facilities on the Council network. Excessive use of on-line banking or shopping may result in access being blocked.
- Using search engines such as google and bing can accidentally direct users to inappropriate websites whose content could not have been foreseen. Care should be taken at all times whilst using search engines and it is not always appropriate to try every link a search engine generates.
- On line streaming of media is not permitted, unless necessary for work reasons due to the bandwidth such sites use. Examples of online streaming media include BBC iPlayer, ITV Player and radio broadcasts.
- On line streaming of live sporting events is prohibited due to the bandwidth such sites use. Examples include Wimbledon, Cricket, World Cup etc.
- Unauthorised use of Social Media applications is prohibited. Authorised use is only available where such sites improve communications with citizens and are in the interests of the Council. Such sites include facebook, twitter, yammer, myspace, bebo, linkedln, ning, flickr, photobucket, youtube, wordpress, blogger, digg.
- Chain letters, junk e-mail or similar correspondence should not be forwarded on either internally or externally. This includes such items as virus warnings and charity correspondence. Any email asking you to forward to all your contacts or send to ten people you know should be deleted with no further action.
- All users should be mindful that non-verbal clues to your meaning are lost in email communication and there is potential for misunderstanding – what's funny to you may appear rude and offensive to a recipient who only has your text to go off.
- Trust your instincts – it's very tempting to reply instantly to emails, but if you've composed a message and your 'gut feeling' tells you not to send it, for whatever reason - don't! Think about the matter further before committing yourself. In particular, venting rage by email is no more acceptable than shouting in someone's face and sarcastic or angry emails sent in haste are likely to be regretted.
- Use of the facilities is for the designated authorised user only. The facilities are not to be used by relatives or spouses.