WYRE FOREST DISTRICT COUNCIL

INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICIES AND GUIDELINES

November 2005

CONTENTS PAGES

SECTION 1

WYRE FOREST DISTRICT COUNCIL

THE INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECURITY POLICY

1. PURPOSE

1.1 This document sets out Wyre Forest District Council's policy towards Information and Communications Technology (ICT) Security so that users (employees, external partners and members) can make effective and appropriate use of these resources.

1.2 The Council has a large investment in the use of Computers and Information Technology (I.T.), which is used to the benefit of all divisions and services. In many areas of work the use of data and I.T. is vital and must be protected from any form of disruption or loss of service. Data stored in the information systems of the Council represent an extremely valuable asset, essential to the effective and continuing operation of the Council.

1.3 It is essential that the availability, integrity and confidentiality of the I.T. systems and data be maintained at a level that is appropriate for the Council's needs.

1.4 The distribution of any information using the Council's computer resources may be subject to management scrutiny and monitored covertly.

1.5 The Council reserves the right to withdraw or limit users access to Computer and I.T. resources.

1.6 The Council has a policy on the use of the Internet and E-mail so that users can make effective and appropriate use of these services. (See Section 3)

1.7 This policy is an update on the policy approved in 2001.

2. OBJECTIVES

2.1 There are four objectives of this policy:

- to ensure that all of the Council's computers and I.T. assets, users, equipment, information and data are adequately protected on a cost-effective basis against any action that could adversely affect the I.T. services required to conduct Council business
- to ensure that users are aware of and fully comply with all relevant legislation
- to create and maintain within all Divisions a level of awareness of the need for I.T. security to be an integral part of the day to day operation so that all users understand the need for I.T. security and their own responsibilities
- to ensure that data is available only to those authorised to see it.

3. APPLICATION

3.1 The security policy is relevant to all Computer and I.T. services irrespective of the equipment or facility in use and applies to:

- all employees and members
- employees and agents of other organisations who directly or indirectly support or use the Computer and I.T. services

- all use of I.T. throughout the Council

3.2 Users may use the Council's Computer and I.T. resources in connection with their work and approved training.

4. RESPONSIBILITY FOR SECURITY

4.1 "Head of Service/Chief Officer" shall be deemed to include the Chief Executive and Heads of Service as appropriate.

4.2 Computer and I.T. security is the responsibility of the Council as an entity and of all employees and members.

4.3 Internet and e-mail security is the responsibility of the Head of Human Resources. The security standards for the firewall configuration are the responsibility of the ICT Manager.

4.4 This policy will apply to all users of computer facilities whether these are network, Personal Computer (P.C.), laptop users, PDAs or Mobile Phones.

4.5 Guidelines follow in Section 2 to assist all users in their compliance with this policy.

4.6 Financial Regulation 19.1 states that Chief Officers shall be responsible for the security of all assets under their control and shall consult with the Head of Financial Services where security is thought to be defective or where it is considered special security arrangements are needed.

4.7 It is the responsibility of each Head of Service to ensure that no unauthorised users including former employees and ex-members are allowed access to the Council's Computer and I.T. facilities.

4.8 It is the responsibility of each Head of Service in conjunction with the ICT Manager to ensure that regular backups are performed and up to date copies held in appropriate locations.

4.9 It is the responsibility of Members to comply with the terms and conditions for the loan of the ICT equipment.

5. LEGISLATION

5.1 The Council has to comply with all relevant legislation affecting I.T. All users of Computer and I.T. facilities must comply with the following Acts and may be held personally responsible for any breach of current and future legislation undertaken knowingly.

5.2 Examples of the current legislation are:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Data Protection Act 1998 and 1984
- Health & Safety at Work Act 1992
- Race Relations Act (1976) & Sex Discrimination Act (1976)
- Criminal Justice and Public Order Act 1994 and Obscene Publications Act (1959 & 1964)
- Human Rights Act 1998 (operative October 2000)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Electronic Communication Act 2000

A summary of these requirements is given in Appendix A.

6. STANDARDS AND PROCEDURES

Physical Access

6.1.1 Precautions should be taken to ensure access to PCs and laptops is restricted at all times to personnel authorised by their Head of Service.

6.1.2 Equipment should be sited to reduce the risk of damage, interference and unauthorised access.

6.1.3 All computer equipment must be included on the Council's inventory and where deemed necessary by the Head of Service additional security arrangements made, for example etching. The ICT Section maintains a central inventory of all computer equipment.

6.1.4 I.T. asset tags are placed on all IT equipment by the ICT Section and should not be removed.

6.1.5 Where computer equipment is removed from Council premises, for example for use at home:

- prior approval in writing should have been obtained from the section head specifying the reason for removal and the duration. It is the responsibility of management to ensure the timely return of all equipment and that no damage has occurred: and
- all of the provisions of this policy document equally apply

6.1.6 No equipment purchased, leased or hired by a department may be connected to the network or attached to any equipment connected to the network without authorisation from the ICT Manager. This restriction also applies to any equipment not owned, leased or hired by the organisation.

6.1.7 Each P.C., notebook, laptop computer, PDA and mobile phone shall have a designated user as agreed by the Head of Service. This designated user is responsible for the overall security of that piece of hardware and associated peripherals. If usage is shared between users then one user should be designated the user.

6.1.8 No office-based equipment should be relocated without consultation with the ICT Section.

6.2 Software access

6.2.1 Requests to provide access to the network and application systems should be made in writing, by the appropriate Head of Service, to the system administrator and ICT Section. The request should detail employee, system and the level of access required.

6.2.2 System administrators are authorised by the appropriate Head of Service for the systems under their control. They are responsible for ensuring the security of their systems is maintained by:

- controlling the issue of passwords;
- procedures for the back up of systems and related data;
- ensuring upgrades or new releases of software are installed and tested in a non-live environment in conjunction with the ICT Section.

6.2.3 Proper mechanisms should be in place to notify system administrators and the ICT Section of all leavers who are users to facilitate the prompt removal of all access rights.

6.2.4 Boot passwords should be set on laptop/notebook PCs that are portable and less physically secure. Boot passwords may be known by several users within an office to enable them to access the P.C. Adequate mechanisms should exist to ensure that access to a P.C. by

authorised personnel could always be achieved. The system administrator should regularly test these procedures.

6.2.5 PCs should not be left "logged in" when unattended.

6.2.6 A screensaver providing immediate complete screen confidentiality should be used in conjunction with a password. This should be set to activate after a maximum duration of 10 minutes.

6.2.7 Passwords should be specific to individual users and comprise a minimum of 6 alpha/numeric characters arranged in such a fashion, as they will not be easily guessed.

6.2.8 Passwords should be used to protect all systems. Users should keep their passwords secret, not be written down and never disclosed to others. Users will be held liable for any misuse of a computer resulting from use of their password/user name. Users should not make use of or attempt to discover another user's ID and password.

6.2.9 It is the responsibility of the system administrator to ensure that there are adequate procedures in place to gain access to the system in case of the absence of employees from the office.

6.2.10 Passwords will be changed to a previously unused password every 90 days.

6.3 Information

6.3.1 Information held on the Council's I.T. facilities or subsequent output, for example printed letters/tabulations, is the property of the Council. Users should have due regard to the provisions of legislation. (See Appendix A)

6.3.2 It is the responsibility of the Head of Service to ensure that systems are in place to meet the legislative requirements (See Appendix A) and the Council's record management policy.

6.3.3 All users including those contracted third parties working for the Council must observe the utmost care and attention in dealing with personal information. In no circumstances must any information about the Council, employees, or its customers be divulged to anyone outside the authority, without proper authority.

6.3.4 Information held should only be released to authorised persons. I.T. facilities supplied must only be used for authorised purposes. Where I.T. facilities are used for personal activities these must not prejudice or interfere in any way with the organisation's I.T. facilities or its business activities.

6.3.5 Any personal or sensitive data displayed upon unattended equipment (visual display units; printed output and computer produced media such as microfiche.) must be protected, particularly in a public area, to ensure it may not be seen by anyone unauthorised to do so.

6.3.6 All computer paper output no longer required by the Council should be disposed of with due regard to sensitivity. Confidential output should be disposed using the confidential waste collection facility and receipts obtained.

6.3.7 Redundant floppy disks, CDs and DVDs containing data must be confidentially disposed of after having received advice from the ICT Section.

6.4 Virus Protection

6.4.1 All PCs (including laptops/PDAs) are protected by virus detection software, which is subject to regular updates to guard against new viruses. Where it is suspected that a file, which has been accessed, may contain a computer virus, including via usage of the Internet, the user should immediately stop using the computer and contact the ICT Section of the Council immediately for assistance. Do not switch off the computer until advised by the ICT Section.

6.4.2 All disks/CD-ROMs must be virus checked prior to use in any of the organisation's computers from whatever source.

6.4.3 Disks/CD-ROM's must not be inserted into PCs until after the boot password has been entered and the computer has either reached:

- the point where you log into the network
- the windows screen on stand-alone computers.

6.4.4 The ICT Section reserves the right to delete suspect e-mail. E-mails containing inappropriate material or references, or containing attachments, which are inappropriate, or contain viruses, may be blocked at the Firewall. The ICT Section may investigate these contraventions of policy and will refer these to Internal Audit for investigation.

6.4.5 The deliberate introduction of any damaging virus is an offence under the Computer Misuse Act 1990.

6.5 Software copyright

6.5.1 The copying of proprietary software programs or associated copyrighted documentation is prohibited, is an offence and could lead to personal criminal liability with the risk of a fine or imprisonment.

6.5.2 The loading of proprietary software programs for which a licence is required but not held is prohibited and this is also an offence that could lead to a large fine or imprisonment. All software systems disks and licences should be recorded in the inventory and securely held in the division.

6.5.3 Personal software should not be loaded on to Council computers under any circumstances. If the software is deemed to be of use to the Council then it should be duly acquired under licence.

6.5.4 Users must not download software from the Internet unless authorised in writing by the appropriate Head of Service in accordance with the Council's Internet and E-mail Policy. Any software downloaded from the Internet must have a direct Council business use and arrangements made to have such software properly licensed without delay.

6.5.5 Unauthorised software i.e. software not belonging to the Council or games software is prohibited from being run or installed on Council equipment.

6.6 Computer misuse

6.6.1 All users should be aware of their access rights for any given hardware, software or data and should not experiment or attempt to access hardware, software or data for which they have no approval or no need to conduct their duties.

6.6.2 Users must not use Council equipment :

- to break through security controls whether on the Council's equipment or on any other computer system
- to intentionally access or transmit computer viruses and similar software
- to intentionally access or transmit information about, or software designed for breaching security controls or creating computer viruses

6.7 Contingency planning

6.7.1 Security copies (back ups) should be taken at regular intervals dependant upon the importance and quantity of the data concerned.

6.7.2 In the case of networked personal computers the prime copy of all data files must be held on the network file server. For stand-alone computers back ups should be by disk or alternative back-up media.

6.7.3 Arrangements must be made by the Head of Service in conjunction with the ICT Section for services with critical systems/operations to be able to continue in the event of complete computing failure.

6.7.4 Security copies should be stored away from the system to which they relate in a restricted access media proof safe. Security copies should be regularly tested to ensure that they enable the system/relevant file to be re-loaded in an emergency.

6.7.5 Security copies should be clearly marked as to what they are and when they were taken. Depending upon the system concerned they should provide for system recovery at various different points in time over a period of several weeks.

6.7.6 Latest versions of application software should be stored in a separate location or by the ICT section.

6.8 Acquisition and disposal of ICT Equipment

6.8.1 All acquisitions should be in accordance with the provisions of the Council's I.C.T. strategy, Financial Regulations and Standing Orders relating to Contracts. Prior to acquisition the I.C.T. Manager should approve the specification of all acquisitions to ensure corporate compatibility of systems and networks.

6.8.2 The disposal of ICT equipment, computer media output containing personal or sensitive data is the responsibility of the ICT Section.

6.8.3 Prior to the disposal of any ICT equipment the Head of Service in conjunction with the ICT Section should ensure that there has been permanent removal of all data and programs.

6.8.4 Disposals should be in accordance with the provision of the Financial Regulations.

6.9 Suspected security incidents

6.9.1 It is the duty of all users to report any suspected security incidents or weaknesses in security to their Head of Service and the Internal Audit section immediately for consideration of any future action that may be necessary.

6.9.2 The Council has adopted a Confidential Reporting Policy, (Whistleblowing policy) which is available on the Intranet and enables users to report suspected breaches of this policy.

7. VIOLATIONS

7.1 Violations of this security policy may include, but are not limited to, any act that:

- exposes the organisation to actual or potential monetary loss through the compromise of ICT security
- involves the disclosure of confidential information or the unauthorised use of corporate data
- involves the use of data for illicit purposes, which may include violation of any law, regulation, or any reporting requirement of any law enforcement or government body.

Any user who has knowledge of a violation of this Information and Communications Technology Security policy must report that violation immediately to their supervisor.

8. BREACHES OF POLICY

8.1 Any user who contravenes any section of this policy will be subject to the Council's disciplinary procedures including where appropriate gross misconduct which could result in dismissal or breach of member's code of conduct. Violations such as the use of unauthorised software, the use of data for illicit purposes or the copying of software, which breaches copyright agreements, will be considered gross misconduct. Any such matters may also be reported to the proper authorities with a view to prosecution of the user.

8.2 Users who are not employees or members of the Council and contravene any section of this policy will be reported to the external partner and such action could result in jeopardising the termination of partnership agreements.

APPENDIX A

Computer Misuse Act 1990

- The Computer Misuse Act, 1990 was introduced to deal with three specific offences that were not adequately covered under existing laws;
- Unauthorised access or attempt to access computer material (such as 'hacking'). Under this offence it is not necessary to prove the users intent to cause harm;
- Unauthorised access with intent. For example, hacking is carried out with the intention of committing a more serious crime such as fraud. Under this offence, if a plan has been hatched which involves the unauthorised use of a computer, the unauthorised use will be sufficient to prove an attempt to commit the crime;
- Unauthorised modification. This part of the act makes it an offence to intentionally cause unauthorised modification such as the introduction of viruses.
- The intention of the act is to enable an organisation to take legal action to protect their data and equipment from unauthorised access and damage.

http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Copyright Designs and Patents Act 1998

- Under this Act, any duplication of licensed software or associated documentation (e.g. manuals) without copyright owner's permission is an infringement under copyright law. All proprietary software manuals are usually supplied under licence agreement, which limits the use of the products to specified machines and will limit copying to the creation of backup copies only. However in some instances, site licenses, permitting the use of software on all machines within a specified site are obtainable.
- To combat the problems of illegal copying, software suppliers have formed their own organisation to police the use of software throughout the UK. The 'Federation Against Software Theft' (FAST) is able to conduct 'spot' checks on organisations, including local authorities, under a court order and without prior warning.
- According to the Act, individuals found to be involved in the illegal reproduction of software may be subject to unlimited civil damages and to criminal penalties including fines and imprisonment.

http://www.fast.org.uk/

http://www.hmso.gov.uk/acts/acts1998

Data Protection Acts 1984 and 1998

- Computers are in use throughout society – collating, storing, processing and distributing information. Much of the information is about people – 'personal data'. This is subject to the Data Protection Acts.
- The Council is only allowed to record and use personal data if, under the Acts, there is a legitimate purpose for doing so and if details for the

information, its use and source have been registered with the Data Commissioner. There are strict rules about how the information is used and to whom it is disclosed.

- The Act gives rights to individuals about whom information is recorded on computer and in certain manual files. They may request copies of the information about themselves challenge it if appropriate and claim compensation in certain circumstances.
- If there is any doubt about whether the information can be collected, used or disclosed please address queries to the Council's designated Data Protection Officer.
- A separate policy document covering the responsibilities under the Act is available via the Council's Intranet site or from the Data Protection Officer direct.

Health & Safety at Work Act 1974

- The Council shall ensure, through the appointed Risk Management Advisor that all ICT equipment is located and used in such a way to not impede health of users or others.
- A separate policy document covering the responsibilities under the Act is available via the Council's Intranet Site.

Defamation

- Facts concerning individuals or organisations must be accurate and verifiable. Views or opinions must not portray their subjects in any way, which could damage their reputation.

Race Relations Act (1976) & Sex Discriminations Act (1976)

- Accessing or distributing material, which might cause offence to individuals or damage the Council's reputation, is forbidden. For example pornographic, racist or sexist material.

http://www.homeoffice.gov.uk/docs/racerel1.html

Criminal Justice and Public Order Act 1994, and Obscene Publications Act (1959 & 1964)

- To ensure this law is complied with, any use of Wyre Forest District Council's computer equipment for viewing, reading, downloading, uploading, distributing, circulating or selling any material which is pornographic, obscene, racist, sexist, grossly offensive or violent is strictly forbidden. This is irrespective of laws regarding the material in the country of origin.

http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_25.htm

Human Rights Act 1998 (operative October 2000)

- Under this Act, everyone has a right to respect for their private life, their home and correspondence, which is commensurate with the need to protect the Council from fraud, introduction of viruses or breach of other overriding considerations. To this end, the Council reserves the right to monitor usage of PC's and telephones.

- Individuals using the Internet, e-mail or telephone should respect the confidence of the Council and colleague's information in disclosing it to other people. E-mail, in particular, should not be circulated in a tone, which may give rise to a claim of inhuman or degrading treatments.

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Freedom of Information Act (2000)

- Any person making a request for information to a public authority is entitled:

  (a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and

  (b) if that is the case, to have that information communicated to him/her.

Electronic Communication Act 2000

- The main purpose of the Act is to help build confidence in electronic communications. The Act creates a legal framework for electronic commerce, It:

  - Clarifies the legal status of electronic signatures;
  - Gives the Government powers to modernise outdated legislation so that the option of electronic communication and storage can be offered as an alternative to paper.
  - Provides a fallback to self-regulatory scheme that will ensure the quality of electronic signature and other cryptography support services.

http://www.hmso.gov.uk/acts/acts2000/20000007.htm

http://www.dti.gov.uk

Regulatory Investigatory Powers Act 2000

- Interception of communications including computer communications such as email, are unlawful unless in accordance with the RIP Act 2000.
- The Council may monitor and record communications for the following purposes:-
- To establish facts and monitor performance of standards.
- In the interests of national security.

- To deter crime.
- To detect unauthorised use of the system.
- To secure a system.

http://www.homeoffice.gov.uk

SECTION 2

WYRE FOREST DISTRICT COUNCIL

GUIDELINES ON THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY POLICY

INDEX

WYRE FOREST DISTRICT COUNCIL

GUIDELINES ON THE INFORMATION AND COMMUNICATIONS TECHNOLOGY GENERAL SECURITY POLICY

1. Introduction – Reasons for Security

The aim of these guidelines is to make users (employees, external partners and members) of the Council's computing facilities aware of the need for adequate security. The Council's computing facilities include all types of computer equipment whether Personal Computer (PC), laptops, network or stand alone PC based systems and PDAs include making use of output from computerised systems.

For full details of the Council's policy on Information and Communications Technology Security please refer to the policy document.

Before using Council Computer resources ensure YOU are appropriately authorised by your supervisor/manager/Head of Service.

The Council has a large investment in the use of Computers and ICT. In order to ensure services can be continued these assets together with the data stored in the information systems must be subject to adequate security.

The Data Protection Acts establish certain rights in relation to the personal information held about individuals in the files on any of the Council's computers. Misuse of this information (whether intentionally or as a result of an accident) could cause damage or distress to those individuals whose data is recorded.

The Council has adopted a policy regarding the use of the Internet and E-mail together with user guidelines. These documents should have been issued to you, if not please ask your supervisor/manager/Head of Service for copies.

2. Security Responsibilities

Heads of Service are primarily responsible for the proper use, security and insurance arrangements for computer equipment, associated software and data under their control. Heads of Service being the Chief Executive and Heads of Service as appropriate.

It is YOUR responsibility to comply with the Council's policy on Information and Communications Technology Security and act in accordance with the authority and instructions issued by your supervisor/manager/Head of Service.

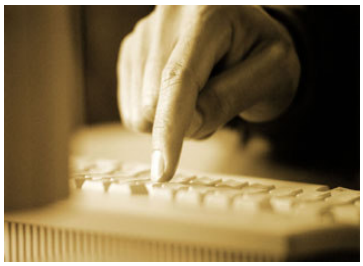
Inventories

Ensure that all computer equipment is recorded in your section's inventory including its description, serial number and location. If a PC is used by several users then one user should be designated as responsible for its house-keeping tasks including back ups.

Physical Security of Computer Equipment and accessories

- Site PCs to avoid the possibility of confidential information being seen by unauthorised persons
- Keep computer equipment secure
- Do not remove computer equipment or accessories from Council premises unless authorised by your supervisor/manager/ Head of Service
- Ensure regular backups are taken.
- Keep back up copies of data in a secure environment away from the originating equipment

Passwords



- Use all password facilities available on the computer
- Do not write passwords down or display them adjacent to the equipment
- Change passwords regularly and immediately an employee leaves the Council or is transferred to another department
- Do not disclose your password
- Do not attempt to use another person's password
- Passwords should not be able to be easily guessed and be a minimum of six characters including numerals

Computer Output

- Computer output must only be released to authorised users
- Output should be kept for the time required by statute or as stated in the Council policy on the retention of documents
- Waste output must be disposed of with due regard to the sensitivity of the information it contains
- Only essential paper computer output should be made, for example for file or record purposes.

3. Basic PC Principles

General

- Stand alone PC based systems are not covered by the access and security procedures provided by mainframe or server linked systems
- Never switch off a PC when there is a disk or CD-ROM loaded
- Use meaningful names for files to avoid confusion
- Remove all files that are no longer required
- Do not reformat disks which contain information that is required to be kept
- Never ignore error or fault messages shown on the PC. Report such messages to the ICT Help Desk as soon as they occur
- Do not move a PC when it is switched on

Back Up Data

- Save work regularly when working on a current file
- One user should be designated responsible for the back up procedure on a Server by the supervisor/manager/Head of Service
- Store back up disks in a secure location e.g. media proof safe in a different location to the server
- Use read/write tab labels on disks to protect the data being overwritten
- Keep a log of the back ups taken
- The frequency of back ups depends on the data maintained
- Ensure data on laptops is backed up regularly to a server

PC Commands

Always:

- Check commands before pressing enter/return
- Exit applications and systems properly
- Check that you are accessing the correct disk and using the correct file directory and name BEFORE deleting a file
- Log out of systems when leaving the PC unattended
- All new software should be loaded by the ICT Section or in the case of major applications, the supplier in conjunction with the ICT Section.

Viruses

- A Computer virus is a computer program that can, once it has infected a PC, cause disruption e.g. damage the data and software on the PC
- A virus once on the PC's hard disk replicates itself onto any disks used to transfer data or software and used for back ups

- Viruses are most commonly found on demonstration and game disks.
- The Internet has introduced a new source of viruses. Bulletin boards are notorious for causing virus attacks as are files downloaded from the web, which are opened without virus checking first.
- Demonstration disks should only be used once they have been checked for viruses. Check with your manager/supervisor/Head of Service for the virus checking arrangements in your section
- Games must not be used on the Council's equipment
- If you think a virus has infected your PC take the following action:
  Stop using your machine. DO NOT turn it off. Contact the ICT section. Put a notice on the machine to make everyone aware. Keep suspect disks and mark them accordingly.
  DO NOT transfer data or programs onto another PC from the one suspected of virus inspection. Such action will prolong the recovery process
- A virus attack can result in loss of service and is not always easily resolved.

BE WARNED AND BE AWARE OF THE RISKS

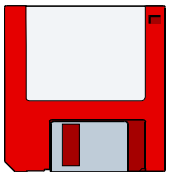
4. Environmental Issues

The PC work location presents many hazards, which should be considered.

Location of Equipment

- Keep the equipment away from temperature, water and magnetic sources e.g. radiators
- Allow air to circulate and keep the air vents free
- Do not place plants or books on the equipment
- Keep your drinks at a safe distance
- Attempt to fix problems only if you know what you're doing. If in doubt contact the ICT Help Desk
- Health & Safety information is shown on the Council's intranet site

5. Care of Disks and CD-ROMS



- Handle with care.
- Insert disks and CD-ROM carefully
- Place CD-ROM's in their case when not in use
- Keep away from magnetic fields and at a comfortable temperature

6. Use of Computer Software

Wyre Forest District Council licences the use of computer software from a variety of outside companies. The Council does not own this software or its related documentation and unless authorised by the software developer, does not have the right to copy it in any way.

According to UK copyright law illegal reproduction of software can be subject to civil damages with no financial limit and criminal penalties, including fines and imprisonment. Wyre Forest District Council does not condone the illegal duplication of software. Officers who knowingly make, acquire or use unauthorised copies of computer software may be subject to the normal disciplinary process including gross misconduct.

Each department should record its software purchases and hold its licences in a secure location.

Officers learning of any misuse of software or related documentation within the Council must inform their supervisor/manager/Head of Service without delay.

7. Misuse of Computer Resources

- Users may use the Council's Computing resources in connection with their work and approved training
- Council computing equipment may not be removed from Council premises without written authorisation from their section head specifying the reason for removal and the duration.
- It is the responsibility of management to ensure the timely return of all equipment and that no damage has occurred. The provisions of the ICT Security policy and these guidelines equally apply under such circumstances
- No equipment may be connected to the computer network in a division without authorisation from the ICT manager.
- Deliberate unauthorised access to, copying of, alteration or deletion of programs and data is regarded as a breach of the Council's ICT Security policy and will be dealt with under the Council's existing disciplinary procedures.
- Computer consumables, for example, disks, paper, printer toner must not be used for personal use.

USING THESE GUIDELINES WILL HELP YOU COMPLY WITH THE COUNCIL'S POLICY ON INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY

If you need assistance with these guidelines speak to your supervisor/manager /Head of Service.

SECTION 3

WYRE FOREST DISTRICT COUNCIL

THE INTERNET AND E-MAIL POLICY

1. PURPOSE

1.1 This document sets out Wyre Forest District Council's policy towards the use of the Internet and electronic mail (E-mail) so that users (employees external partners and members) can make effective and appropriate use of these services.

1.2 The Internet is a very useful form of communication, but it is not risk free. It is essential that good management practices be put in place detailing responsibility and guidelines on its use to ensure that access is justified and cost effective.

1.3 The Council reserves the right to withdraw or limit users access to Internet and e-mail services.

1.4 It is essential that standards relating to accessing appropriate content and maintaining the good reputation of the Council are observed.

1.5 This policy is an update of the policy approved in 2001.

2. MONITORING

2.1 The Internet and E-mail services are installed expressly for the purpose of supporting the Council's business. To maintain security and integrity the Council reserves the right under the Regulation of Investigatory Powers Act to investigate monitoring logs for the purpose of:

- Detecting viruses
- Prevention of unauthorised access to Council systems
- Inappropriate use of the Internet and E-mail as defined by this policy
- Detecting unusual trends in the use of Internet or e-mail services.

2.2 The monitoring is covert and includes the automatic blocking and monitoring of flow and content of communications such as:

- blocking access to certain internet sites, particularly those that might contain offensive sexual, racist or violent images
- monitoring of e-mails, by content, size of attachments or graphic/animations files
- monitoring large-scale circulation of e-mails, which might make the system less effective and run less smoothly.

2.3 The Council will follow the guidance issued by the Information Commissioner on Monitoring at Work.

2.4 Users will retain the right for confidentiality in making personal communications, which are not subject to monitoring under this policy i.e. telephone conversations, written memoranda.

2.5 Users should be aware that it is not possible to differentiate between business and personal use. All usage may be subject to monitoring.

3. ACCESSING INFORMATION ON THE INTERNET

3.1 "Head of Service" shall be deemed to include the Chief Executive and Heads of Service as appropriate.

3.2 Users must avoid spending excessive time accessing the Internet.

3.3 Private usage should not be at the expense of Council time or Council resources e.g. paper, disks, printer toner.

3.4 The Council's Internet service and e-mail may not be used for transmitting, retrieving or storing any communication of a discriminatory or harassing nature or materials that are offensive, obscene, pornographic, sexually explicit, racist, defamatory, depicts or incites violence or is otherwise illegal. Should there be evidence of any abuse of this nature disciplinary action will be taken.

3.5 Users must not use Council equipment and/or a Council Internet account:

- to break through security controls whether on the Council's equipment or on any other computer system
- access Internet traffic including E-mail not intended for them, even if not protected by security controls
- intentionally accessing or transmitting computer viruses and similar software
- intentionally accessing or transmitting information about, or software designed for breaching security controls or creating computer viruses
- to access inappropriate interactive sites such as gambling or dating agency sites.

3.6 Prior approval should be obtained from the Head of Service before subscribing to any bulletin boards, mailing list or newsgroup.

3.7 When participating in discussions in newsgroups and mailing lists or using bulletin boards, users may offer information and advice to others if that is appropriate to the job, or if the value received from the discussion represents a reasonable return for the time and effort involved.

3.8 Employees must not participate in discussions of politically controversial matters, whether national or local.

3.9 Users must not give advice or information known to be contrary to the Council's policies or interests.

3.10 Users must ensure that any information shared with external organisations or individuals does not include:

- reference to Exempt information contained in committee reports; and/or
- any confidential personal information (officer, member or otherwise) having due regard to the Data Protection Acts 1984 & 1998

Any exception to the requirements of this paragraph requires specific authorisation in writing from the appropriate Head of Service.

4. PUBLISHING DATA ON THE INTERNET – COUNCIL'S WEB-SITE

4.1 Data published on the Internet is available worldwide, including countries, which have no data protection legislation.

4.2 One officer, the Information & E-Government Officer is responsible for collating the content of the Council's web-site. The information on the site must remain up to date and procedures for routine maintenance should be laid down in each division to provide this information to this officer. Each Head of Service is responsible for the accuracy and compliance with Data Protection and Copyright legislation of information available on the Internet relevant to their areas of

responsibility together with any links from their web pages to other pages on the Internet.

4.3 No personal data may be published on the Internet unless:

(a) such use of data has been properly registered; and

(b) the individuals concerned have given their written consent to the worldwide disclosure of their personal data in compliance with the Data Protection Acts 1984 & 1998.

4.4 Any information included in the Council's web-site must not include:

- reference to Exempt information contained in committee reports; and/or
- any confidential personal information (officer, member or otherwise) having due regard to the Data Protection Acts 1984 & 1998.

Any exception to the requirements of this paragraph requires specific authorisation in writing from the appropriate Head of Service.

4.5 All published Web pages should have a link to the Council's disclaimer.

5. PLACING ORDERS FOR GOODS AND SERVICES

5.1 Orders for the provision of goods and services to the Council can only be placed via the Internet when in accordance with the Council's approved methods of procurement as detailed in the Council's constitution and in compliance with the Council's Procurement strategy.

5.2 Users who place orders for goods/services not in accordance with 5.1 will be personally liable for all costs involved in the transaction and should not be made at the expense of Council time and resources.

6. COPYRIGHT INFRINGEMENT

6.1 Any copyright infringement could have severe cost implications for the Council.

6.2 Users must not download software from the Internet unless authorised in writing by the appropriate Head of Service in accordance with the Council's Computer Security Policy.

6.3 When downloading files from the Internet or when copying or attaching text to E-mail there may be a risk of copyright infringement. Users should not copy information originated by others and re-post it without permission, or at least acknowledgement of, the original source.

6.4 Users must not transmit copyright software from their computer to the Internet or permit anyone else to access it on their computer via the Internet.

6.5 If a user is to place reliance on information posted on the Internet then the user must not assume that it belongs to the person or organisation it appears to without checking by another means, for example telephone.

7. VIRUSES

7.1 Virus protection software is provided on all Council ICT equipment with access to the Internet. Where it is suspected that a file which has been accessed on the Internet may contain a computer virus, the user should immediately break the connection, stop using the computer and contact the ICT Section of the Council immediately for assistance.

7.2.1 Deliberate introduction of any damaging virus is an offence under the Computer Misuse Act 1990.

8. **E-mail**

8.1 E-mail is the electronic transfer of information, either internally between users, or externally between Wyre Forest District Council users and outside organisations or individuals. It can be informal in nature or it can be an official record of a decision or action.

Under English law contracts can be established in any form the parties choose, whether in writing, orally or through an exchange of E-mail messages. E-mails produce a potential evidential record that is absent in telephone conversations.

8.2 Appropriate Use of Electronic Mail (E-Mail)

8.2.1 As e-mail (external & internal) has become a major route of communication it must be ensured that an appropriate and timely response is made to messages received via this medium. Users should make arrangements to respond in periods of their absence.

8.2.2 Users should be aware that E-mail, in the same way any other form of communication represents and reflects on the Council, regardless of any disclaimer included in messages. The message should be clear and easy to understand. Users must comply with the Council's guidelines on the use of E-mail.

8.2.3 The transmission of E-mail, which conflicts with the interests of the Council or contravenes the Council's policy on ICT Security or contravenes the Data Protection Acts 1984 & 1998 or other legislation is expressly prohibited.

8.2.4 E-mail should not be used for formal communications where a permanent record should be kept. Advice given by E-mail has the same legal bearing as any other written advice.

8.2.5 Users must not send unsolicited, irrelevant or inappropriate E-mail or participate in chain or pyramid letters or similar schemes.

8.2.6 Users must not use E-mail either internally or on the Internet; to harass or threaten anyone in any manner or to abuse anyone, even in response to abuse directed at them.

8.2.7 Users must not use E-mail to distribute unauthorised material, for example, material that is considered illegal, offensive and vulgar.

8.2.8 Users must not use anonymous mailing services to conceal their identity when mailing through the Internet, falsify E-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, E-mail address or other details.

8.2.9 Users may use E-mail for occasional personal use (but not for private business activities) provided not at the expense of Council time. Users must understand that any personal use does not guarantee privacy of correspondence.

8.2.10 E-mails addressed to 'Everyone' should only be used in exceptional circumstances and solely for official/operational business purposes.

8.2.11 Internal circulars relating to personal/social matters, for example 'Items for Sale' and promotion of Council sporting events, should be communicated via the intranet only.

8.3 Sending E-mail

8.3.1 Personal, confidential or exempt material must not be transmitted by E-mail to individuals other than authorised Council users.. Information transmitted by E-mail either internally or on the Internet is not guaranteed to be secure nor to arrive at their destination within a particular time, or at all, nor is there any control over its onward transmission.

8.3.2 Users must ensure their E-mail communications are accurate, concise, courteous, do not contain any defamatory statements and do not breach any Council policies.

8.3.3 Users must regularly check and respond to incoming E-mail as directed by the appropriate Head of Service. E-mails must be filed or disposed of as appropriate to their contents in accordance with corporate or division filing and retention policies.

8.3.4 The corporate legal disclaimer is shown at the end of all e-mail transmissions. The removal of this disclaimer is prohibited.

9 BREACHES OF POLICY

9.1 Any user who contravenes any section of this policy will be subject to the Council's disciplinary procedures including where appropriate gross misconduct which could result in dismissal or a breach of member's code of conduct. Any such matters may also be reported to the proper authorities with a view to prosecution of the user.

9.2 Users who are not employees or members of the Council and contravene any section of this policy will be reported to the external partner and such action could result in jeopardising the termination of partnership agreements.

SECTION 4

WYRE FOREST DISTRICT COUNCIL

GUIDELINES ON THE USE OF E-MAIL

The aim is to allow maximum access and use of E-Mail with the minimum of restrictions for authorised work purposes. E-Mail is not intended to replace formal word-processed documents nor does it replace the use of the telephone or face to face contact. For full details refer to the policy document.

E-mail and Internet access must only be via the approved Council gateway. Remember e-mail may be convenient but it is also easy to misinterpret without visual clues of face-to-face communications. Also e-mail is easily forwarded with the possibility of being viewed by unauthorised personnel.

Always remember the clarity of the written word. Simple spelling mistakes, capitalised words and the ambiguities of language can easily lead to errors and false assumptions. A short and simple e-mail is more likely to get the recipient's attention. If the message has to be longer use sub-headed short paragraphs to add structure and make it easier to digest.

DO USE E-MAIL FOR

- Short life temporary text
- Draft documents, minutes, agendas etc
- Messages when contact cannot be made by telephone, but reply and forward to only those necessary
- Urgent circulation of documents/requests
- Setting up Proxy access
- Setting up a Rule

DO NOT USE E-MAIL FOR

- Text which might be considered abusive, aggressive, defamatory, obscene, deliberately anti-social, harassing, illegal or otherwise liable to bring the Council into disrepute
- To avoid face to face communications and difficult matters
- Documents which require formal circulation and authorisation
- Comments which you would not normally commit to paper
- Circulating lengthy documents to a large number of people. Where possible publish on the Intranet and e-mail intended audience with the appropriate access address.
- Do not use email for large attachments, i.e. pictures, if in doubt contact the ICT Section
- Documents where hard copy files are required, unless urgent delivery is required
- Sensitive or confidential information
- The sale of personal items, these should be advertised on the Intranet.
- Subscribing to e-mail newsletters which are never read.

NEVER

- Disclose your password
- Leave your P.C. on and open when you leave your office
- Send documents or attachments of excessive size

SECTION 5

Employee/External partner's Acknowledgement of Receipt

All Employees/external partners will need to sign the Acknowledgement ofReceipt before they are connected to Email.

EMPLOYEE'S/EXTERNAL PARTNER'S ACKNOWLEDGEMENT OF RECEIPT OF:

(1) THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY POLICY AND GUIDELINES
And
(2) THE INTERNET AND E-MAIL POLICY

I have received written copies of the Information and Communications Technology Security Policy and the associated Guidelines. I agree to follow these principles. I understand that if I make unauthorised use of Council equipment this could lead to a breach of code of conduct, which could lead to disciplinary action being taken against me including being classed as gross misconduct which could result in dismissal as well as criminal prosecution. I understand the terms of this policy and agree to abide by them.

I have received written copies of the Internet & E-mail Policy and the associated Guidelines. I understand the terms of this policy and agree to follow these principles. I am aware that the Council's security software may record, for management monitoring, the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. Further I understand that any message I send or receive may be recorded and stored in an archive file for management monitoring. I know that any violation of this policy could lead to disciplinary action being taken against me including being classed as gross misconduct which could result in dismissal as well as criminal prosecution. I understand the terms of this policy and agree to abide by them.

Signed: …….. Date: ……

Name: ……..

Post: …….. Division: ……

Please return the completed form to the Head of Human Resources

SECTION 5

Member's Acknowledgement of Receipt

All Members will need to sign the Acknowledgement of Receipt before they are connected to E-mail.

MEMBER'S ACKNOWLEDGEMENT OF RECEIPT OF:

(1) THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY POLICY AND GUIDELINES

And

(2) THE INTERNET AND E-MAIL POLICY

I have received written copies of the Information and Communications Technology Security Policy and the associated Guidelines. I agree to follow these principles. I understand that if I make unauthorised use of Council equipment this could lead to a breach of code of conduct. I understand the terms of this policy and agree to abide by them.

I have received written copies of the Internet & Email Policy and the associated Guidelines. I understand the terms of this policy and agree to follow these principles. I am aware that the Council's security software may record, for management monitoring, the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. Further I understand that any message I send or receive may be recorded and stored in an archive file for management monitoring. I know that any violation of this policy could lead to a breach of code of conduct and criminal prosecution. I understand the terms of this policy and agree to abide by them.

The Chief Executive may, at his discretion, authorise the return of ICT equipment where there has been a breach of these policies and require the reimbursement of any costs incurred by the Council in respect of inappropriate use.

Signed: …….. Date: ……

Name: ……..

Post: …….. Division: ……

Please return the completed form to the Head of Human Resources, Member Services Division, 7/8 New Street, Stourport-on-Severn DY13 8UL.