

PROTOCOL FOR THE USE OF ICT EQUIPMENT AND SERVICES

The protocol and its procedures that follow are in force for a number of reasons, the most important of which are:

- To protect the Authority and its Members from prosecution. This can involve Data Protection, software usage, security and virus issues.
- To protect the assets owned by the Authority. These assets include not only software and hardware but also data.
- To enable you to carry out your duties safely and more effectively.

Remember this protocol is to help all users of ICT Services and is not intended to restrict you in carrying out your normal council activities.

This protocol will be updated from time to time to take into account any changes. It will be widely distributed either electronically or via hard copy.

Any breach of the protocol should be reported to the Monitoring Officer who will investigate and, depending on the outcome, may report the matter to the Standards Committee if there has been a breach of the Code of Conduct. This could lead to a removal of your access rights and/or the equipment being removed from your possession.

PROCEDURES FOR THE USE OF ICT EQUIPMENT AND SERVICES BY MEMBERS OF THE COUNCIL

1. INTRODUCTION

All Members of the Council should familiarise themselves with these procedures.

1.1 The Council's Policy Statement on use of Information Systems

In summary, the Council's policy is:

The Council's Information Communication and Technology (ICT) infrastructure is an essential business asset and should not be compromised or misused by users.

The full text of the council's policy is available on the Intranet in Personnel Practice Note 47.

2. ICT EQUIPMENT AND SERVICES

2.1 Equipment Provision and its Usage

ICT equipment is provided to help you to carry out your role as a Councillor.

It is permissible for equipment to be used for:

- Council business
- Communicating with staff, members and the public
- Dealing with official correspondence
- Researching relevant issues

It must **not** be used for:

- Party political purposes
- Personal use

2.2 Definition of Party Political Purposes

There is a clear statutory ban on the use of Council property (including PC's, Laptops copiers, scanners, printers, paper and software) **for any purpose connected with party political publicity**, either at election time or at any other time. At election time there are also detailed restrictions on the use of Council property for other party political purposes as well as publicity. The safest course is to avoid the use of Council IT equipment for any purely **party political purpose** at **any** time.

This does not prevent Members from using Council property for **general** "political" purposes, including for example researching an issue which concerns you as a councillor, even though that issue may be politically controversial. Also this does not prevent you from using Council property to work on matters raised by a constituent in your Ward. However, Council property should not be used for processing names and addresses of your constituents for electioneering purposes.

2.3 Systems and Software

The laptop will be preloaded with installed software to enable you to carry out your role as a councillor or carrying out work as an officer of one of the Council's political groups.

All users are given access to the following systems:

- Microsoft Office
- Adobe (PDF reader)
- GroupWise (e-mail)
- The Council's Telephone A-Z
- Intranet
- Internet

Software and systems may change over time. These changes could include access levels, upgrades or replacements.

The ICT Service, will arrange for you to be given access to any other systems you need to carry out your role as a councillor.

3. **USER ID AND PASSWORD**

Access to High Peak Borough Council systems is controlled through **User Identifiers (User IDs)** and **passwords**, which will give you the correct level of access required for your role.

- The ICT Service will assign you a User ID and Password.
- Your password is personal to you, **so keep it secret**.
- It is bad practice to write your password down.
- If others learn your password they can access applications that they may not be authorised to use. **You are responsible** for actions that take place on computer systems where access has been gained using your User ID and Password.
- Passwords can be changed on request, by contacting the ICT Service.

4. **DATA SECURITY**

You are responsible for the computer (laptop) allocated to you and any data it holds.

- Never store personal, confidential or contractual data on your laptop's C: drive. If you do store such data and lose your laptop or it is stolen you may be in breach of the Data Protection Act and/or other legislation Acts.
- If your laptop is lost or stolen, report this immediately to ICT, who will determine what actions need to be taken.
- Make sure that your computer is not left unattended while switched on or while connected to the network.
- If you think that an unauthorised person has accessed your computer you should inform the ICT Service immediately and request a new password.
- If you are dealing with confidential information, make sure that passers-by or visitors cannot see data on your screen or on printouts.

5. **HOUSEKEEPING**

Delete unwanted emails as you go. Do not allow unwanted emails to build up.

Much as a house becomes untidy unless you do housekeeping, you will find your computer disk (C: drive) and the Email Server will fill up with files unless you do some regular housekeeping.

6. VIRUSES

Computer viruses represent a real threat to the continuous functionality of the Council's ICT systems. The Council employs a real time dynamically activated virus checker in order to minimise potential virus attack.

What to do if you find a virus:

- All virus warnings must be notified to ICT services, who will determine what action needs to be taken.

7. SOFTWARE AND AUDITS

All software to be used by the Council will be acquired and installed by the ICT Service. Only software that has been bought by the Council, and is licensed to the Council, can be used on Council computers.

Random electronic audits of HPBC computers, including laptops, are carried out on a regular basis.

Any unlicensed or unauthorised software will be removed.

It is illegal to copy or install software that has not been obtained under the terms of a software licence agreement. The Council could be liable to prosecution if unlicensed software is found on a Council computer.

8. E-MAIL

E-mail communications, either internal or external, are not guaranteed to be private, or to arrive at their destination within a particular time, if at all. There is also no guarantee that the recipients will read them.

E-mail communications, whether external or internal, are the same as any other correspondence and as such should comply with the Council's Customer Care Policy relating to Written Communications (see *Personnel Practice Note : 21*).

You should be careful what you say in your e-mail messages. E-mail communications have the same legal standing as any other written communication. E-mail may be disclosable under the Freedom of Information Act in the same way as any other written communication or document.

Carefully check your e-mail before you send it and do not write anything that you could not explain to a Court or Tribunal.

E-mails that have been deleted may still be recovered for legal purposes

You must make sure that all e-mailed letters, or memos, that contain contractual details or instructions, are backed up by a paper copy, and signed by the author.

Do not print e-mails indiscriminately. Only print those e-mails that you need to keep for file purposes.

You should not pass on material that has been e-mailed to you personally without the permission of the author.

You must not use e-mail:

- to place orders for goods or services
- to copy or transmit software, documents or other information protected by copyright law
- to abuse, threaten or harass others, send defamatory, obscene, sexist or racist messages or jokes, or use inappropriate language.
- to send an electronic chain letter or in any other way publish junk e-mails (otherwise known as Spam)
- for obtaining or sending inappropriate text and images
- for party political purposes

NB. ICT Services may need to open your mailbox for fault finding purposes, or system maintenance and may need to alter your settings if they are found to be causing problems with the mail system as a whole.

9. INTERNET

The Internet is only to be used for legitimate, council-related research, reference or educational purposes.

You must not use, or try to use, the Council's Internet facilities for :

- placing orders for goods and services
- accessing communications intended for someone else
- breaking through security controls on either internal or external computer equipment or giving someone else the information they need to do so
- accessing or transmitting computer viruses or carrying out any activities that could cause congestion or disruption of computer networks and systems
- obtaining or sending inappropriate text and images as specified in 10.4
- infringing copyright laws
- downloading or uploading any document, information or software protected by copyright

- knowingly doing anything which is illegal or unlawful.
- to sign up to inappropriate mailing lists

10. THE LAW

10.1 Data Protection

You are responsible for complying with the Data Protection Act 1998 that covers information held in electronic and paper-based form about individuals.

It is a criminal offence to collect and process personal data on your PC unless the use is registered with the Data Protection Registrar. Details of registration should reflect internet use. Democratic Services and The ICT Service can provide information about the Council's Data Protection registrations and can give you advice.

The Data Protection Act 1998 considerably increases the obligation on users of personal data, such as:

- prohibition on processing certain 'sensitive data' such as someone's marital status or ethnic origin.
- banning sending personal data to non-European Economic Area countries with inadequate protection for data subjects;

The Act requires holders of data about third parties to be responsible for its security.

Failure to secure sensitive information that later becomes compromised could not only affect the Council's image but could lead to litigation against the council and/or yourself.

10.2 Computer Misuse Act 1990

This Act covers unauthorised or malicious use of any computer system.

It is the law used to prosecute hackers and people who write and distribute computer viruses deliberately.

It is a criminal offence to access, or attempt to access, any computer system you are not authorised to access.

This law protects against employees and members of the public who deliberately cause damage to systems and data. The Act also makes it illegal for a person to deliberately delete data or sabotage systems to the detriment of the Council.

10.3 Harassment

You can commit harassment either by using e-mail or sending a harassing message to someone or by downloading and distributing material from the Internet which constitutes harassment because it creates an intimidating working environment. Harassment and discrimination are unlawful under the Protection from Harassment Act 1997, the Sex Discrimination Act 1975, Disability Discrimination Act 2005 and the Race Relations Amendment Act 2006.

As with any form of harassment under the anti-discrimination legislation the intention of the parties is irrelevant. The problem with e-mail is that, with the lack of visual clues, offence may be caused where none was intended.

10.4 Obscene Material

Publishing obscene material is a criminal offence under the Obscene Publications Act 1959. This includes electronic storing and/or transmitting obscene materials that would tend to deprave and corrupt or paedophile material.

10.5 Defamation or false statements

The liability for defamation or false statements applies to electronic communication just as it does to more traditional forms of communication. Anyone who e-mails a libellous or false e-mail message or posts such a message on the Internet will be responsible for it and liable for any damage it causes to the reputation of the victim.

In addition to the liability of the individual who made the libellous or false statement, the Council may also be held liable. This could be either under the normal principles of:

- **Indirect** liability because the Council is considered responsible - known as 'vicarious liability'; or
- **Direct** liability as a publisher because of providing the link to the Internet and e-mail system.

An untrue statement that damages the reputation of a person or company by causing people to think worse of them will generally be defamatory. Similarly, a false statement intended to cause damage to a person or their economic interests can bring a claim for damages.

Computer equipment must not be used to infringe copyright. Copyright laws apply to documents and information published on the web or installed on computers just as they do to magazines or books.

Although any material placed on the Internet or in public discussion areas is generally available, the originator still has moral and, possibly, legal rights over it. You should not copy it without acknowledging the original source and, where appropriate, gaining their permission. This applies even if you modify the content to some extent. Please note that any official material placed on a website is subject to copyright laws.

Copying third party documents without the owner's consent will in nearly all cases constitute copyright infringement, this includes text, graphics, audio and video clips. The most notable exception to this rule is Crown copyright that is not enforced, for example, statutes and printed advice published by the OPSI.

The Council is a signed up member of the Federation Against Software Theft (FAST). Downloading or copying information in breach of copyright and the Council's membership of FAST will be treated as serious misconduct under the Council's disciplinary procedure.

Random checks may be carried out by ICT Services to ensure that no material in breach of copyright is held on Council computers.

10.7 Contracts

E-mail is generally regarded as an informal means of communication but it is, nevertheless, capable of creating or varying a contract in just the same way as a written letter. You should be careful not to create or vary a contract accidentally.

10.8 Disclaimer

Despite putting confidential disclaimers and, where appropriate, personal disclaimers, on external communications, there is still nevertheless a legal connection to the Council. Always remember that any statement you make may still be construed as representing the Council.

11. WORKING AT HOME

Laptops are provided to members for use at home and on Council premises. Health and Safety rules apply at home when working on Council business.