ICT SECURITY POLICY 2008

CONTENTS

1. INTRODUCTION

1.1 Information and Communications Technology (ICT) is an integral part of the Council's activities.

Because IT is essential to the provision of services, policies and procedures need to be laid down and enforced in order to safeguard those services and the Council's interests. These include:

- the physical assets
- access to the information on those assets
- services continuity
- users of the systems and equipment
- compliance with legislation

1.2 This Policy therefore applies to:

- all employees and elected members of the Council
- all employees and agents of other organisations who directly or indirectly support or use the Council's computer systems or networks
- all temporary and agency staff directly employed or indirectly engaged by the Council

1.3 This Policy applies to all areas of IT, including:

• PCs and associated equipment, including personal digital assistants (PDAs) and mobile equipment
• printers and fax equipment
• network communications
• software

2. **ENFORCEMENT**

2.1 All users of the Council's IT equipment are responsible for compliance with this Policy.

2.2 IT security is viewed seriously by the Council and any breach of this Policy could lead to disciplinary action being taken against those who commit this breach.

Breaches may be considered gross misconduct and as such may lead to the dismissal of the employee or employees concerned.

Breaches include:-
• the installation and use of unauthorised software (including screensavers & wallpaper),
• the installation and use of any unauthorised computer or telecommunications equipment,
• unauthorised and/or illicit use of the Internet,
• the use of data for illicit purposes (including breach of any law, regulation or any reporting requirement of any law enforcement or government agency),
• the copying of software which breaches copyright agreements,
• exposing the Council to actual or potential loss (monetary or otherwise) through the compromise of I.T security,
• the unauthorised disclosure of confidential or personal information or the unauthorised use of corporate data,
• unauthorised personal use of equipment or changes to equipment configuration
• unauthorised deletion or alteration of files or data
• avoidable damage to the Council's equipment
• sharing of passwords or otherwise compromising password security

This is a list of examples and is not intended to be exhaustive.

2.3 Any individual who has knowledge of a breach of this Policy must report that breach immediately to his or her line manager. Failure to do so could result in disciplinary action being taken.

2.4 The Clerk is responsible for ensuring appropriate systems are in place to address policy breaches.

3. LEGISLATIVE FRAMEWORK

3.1 The Council and all IT users must comply with all relevant legislation. Users may be held personally responsible for any breach of any relevant legislation.

Relevant legislation includes, but is not restricted to:
Data Protection Act 1998 (see paragraph 5.2 below)
Copyright, Designs and Patents Act 1988
Computer Misuse Act 1990
Health & Safety Act (Display Screen Equipment) Regulations 1992
Freedom of Information Act 2000
Anyone who is unsure of their responsibility should seek clarification from their line manager.

4. USE OF COUNCIL IT EQUIPMENT & NETWORKS

4.1 Access by outside bodies into any of the Council's networks or equipment is not permitted without prior recorded agreement from the appropriate Officer.

4.2 Telephone numbers allowing access to the Council's networks must not be disclosed to unauthorised persons/bodies.

4.3 No equipment may be:
- connected to the network, or
- attached to any equipment connected to the network or which could be connected to the network (e.g. laptops) without prior recorded authorisation from the appropriate Officer.

5. DATA AND PROGRAM OWNERSHIP

5.1 The Council's Data

(a) All computer programs and data resident on the Council's hardware are for the sole use of the council in undertaking its business; access by members and employees is solely for this purpose.

(b) Copying, alteration or interference with computer programs is not permitted, without the recorded agreement of the Clerk.

5.2 Data Protection Legislation

(a) Systems (manual or computer based) which process personal data about living persons must comply with current data protection legislation.. Copies of the official registration - and any subsequent amendments - must be kept in the Council offices

(b) There must be no unauthorised disclosure of personal data. Personal data may only be disclosed by the officers who are responsible for the data, with the express permission of the owner, in accordance with data protection legislation. Disclosures must only be made by and to the parties specified on the Data Protection Registration form and in accordance with current data protection legislation.

(c) Key data protection principles include, but are not limited to:
- Personal data must be processed fairly and lawfully.
- Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes must not be kept for longer than is necessary.
- Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data.

6. ACCESS TO SYSTEMS

6.1 General

The approval, setting up and control of all networks and systems is the responsibility of PCC in conjunction with the appropriate Officer. This includes
- access to the internet, and
- systems which are being accessed from public areas.

Access must be controlled in accordance with procedures approved by PCC.

6.2 **Day-to-day management** of each system may reside outside PCC. The appropriate Officer must be consulted before access can be given to that system. Requests for access to systems will be accepted only from authorised Appropriate Officer.

6.3 Password Controlled Access

(a) Each user must have a unique user-ID and password. The use of another person's user-ID is not permitted. Users must not disclose their user-ID or password or visibly record them on or near equipment providing access to networks or systems.

(b) Users must change default passwords, which enable first access, immediately.

(c) Passwords should be a minimum of 7 characters in length, at least one of which must be numeric and one capital letter. Passwords must be changed at regular intervals and especially when it is suspected that the password has been disclosed. The change should be to a previously unused password.

(d) Persons intending to leave the employ of the Council who have access to systems, must immediately have their access capabilities restricted as appropriate, and removed as soon as possible on leaving the Council, either by the system owners and/or local systems administrators whichever is applicable.

7. PURCHASE AND DISPOSAL OF IT EQUIPMENT AND SOFTWARE

7.1 The authority to purchase equipment is controlled by PCC

7.2 Details of all IT equipment must be kept on a central IT Asset Register and the Pontypool Community Council Asset Register. However, the accuracy of the information is a joint responsibility between PCC and the appropriate Officer at TCBC

7.4 Disposal of any IT and associated equipment must be carried out in consultation with PCC and the appropriate Officer.

8. PCs AND PORTABLE COMPUTERS

8.1 **Configuration** (Set Up)

(a) This includes PCs, and portable equipment such as laptops and handheld devices.

(b) The configuration (set up) of such equipment must be carried out by TCBC

Systems will be configured to allow users access only to those applications, features and facilities they require to perform their day to day duties, and, where possible, these configurations will be standard across workgroups and locked to prevent unauthorised changes

8.2 **Approved Software**

Unlicensed or personal software must not be installed on the Council's hardware, or connected in any way to the Council's equipment or systems. If software is deemed to be of use to the Council then the Council in accordance with section 7 should duly acquire it under licence. Random spot checks may be conducted by Departmental staff.

8.3 **Mobile Media**

Use of the disk drives and USB ports (floppy disks and CDs and any other mobile media) on networked PCs is not permitted unless recorded authorisation has been given by the Clerk. Where authorisation has been given to a specific user it is their responsibility to ensure that all disks inserted do not transmit any viruses onto the Council's network.

Mobile media which has been used on other PCs, networked or otherwise, within or outside the Council, must not in any case be used on PCs connected to the Council's networks, until the media has been checked using appropriate virus checking procedures.

8.4 **Unauthorised Equipment**

Users must not connect unauthorised equipment of any kind to the Council's computer systems or networks.

9. SAVING DATA / BACKUPS

9.1. It is the joint responsibility of users and PCC, to ensure that appropriate back up procedures are operated and tested.

10. SOFTWARE LICENCES

10.1 It is the responsibility of TCBC to advise PCC of the appropriatesoftware licences that need to be obtained and maintained.

10.2 PCC will ensure that, if the Policy laid out in this document is followed, the legal requirements of licences will be met. However, it is the responsibility of the appropriate Officer to ensure that this Policy is followed at all times.

11. ELECTRONIC COMMUNICATION (INCLUDING USE OF INTERNET)

11.1 **Electronic Communication** includes:

- use of E-mail within the Council,
- use of E-mail to and from addresses outside the Council,
- use of the Council's Intranet, and
- general use of the Internet.

11.2 **Authorisation**

Users will be connected to the internet and/ or e-mail only after receipt of a completed and suitably authorised UAR Form.

11.3 Officers must comply with the **Council's Code of Practice** relating to the Use of Internet and Electronic Mail Facilities (reproduced at Appendix 1). The following points should be noted:-

- Services will not be used to access, create, transmit or publish any material likely to cause offence.
- The hardware and software, and all messages belong to the Council; messages can be traced to both sender and recipient.
- The Clerk of the council and TCBC has the right to monitor the content of all e-mails and data which are transmitted to or from the Council's equipment or downloaded to the Council's equipment.
- All Internet sites visited are recorded automatically.
- Current Council personnel policies, including those on equal opportunities and harassment, apply.
- Data Protection legislation applies.
- Failure to comply with Council policies and procedures or legislation may lead to disciplinary and/or legal action.

11.4 **Internet and Intranet Access**

Failure to follow this Policy may put the Council's data and networks at risk: therefore non-compliance may lead to disciplinary action.

(a) Access to the Internet and / or Intranet is only permitted on receipt of a properly authorised UAR form. Control of access will be dealt with in conjunction with TCBC

(b) All access must be in a manner approved by and arranged through PCC.

(c) Any data or information downloaded from the Internet must not be loaded to any other PC, networked or otherwise, until the data has been checked for viruses by Microsoft Forefront.. It is the user's responsibility to ensure that this is done.

12. PHYSICAL AND ENVIRONMENTAL SECURITY

12.1 Everyone has a duty of care to ensure that equipment:

- is not put at risk of damage or theft, and is used in accordance with safe working practices. For example:
- The location of IT equipment should be subject to a risk analysis, and should be sited to avoid unauthorised access, damage, theft interference and the effects of environmental or other hazards.
- Equipment in transit must not be left unattended.
- Equipment must not be removed or moved to another location without notification being given to PCC and the appropriate changes made to the central asset register.
- Eating and drinking should not take place in the immediate vicinity of equipment.

Appendix 1

USE OF INTERNET AND ELECTRONIC MAIL FACILITIES
CODE OF PRACTICE – EMPLOYEES

This document outlines the policy adopted by the Council for the acceptable use of computer network facilities, including electronic mail and the Internet.
Anyone authorised to use such facilities is required to abide by the conditions laid down in this policy. Any breach of these conditions could result in disciplinary action or in some cases a criminal prosecution.

All users are expected to demonstrate a responsible approach in the use of resources available to them, and to show consideration for other users, both those using the Council's facilities and those with whom they may come into contact on the Internet. Users are expected to behave in a legal, moral and ethical fashion that is consistent with Council policies and standards.

It must be recognised that any view communicated over the Internet will be deemed to be the view of the Council, and will in most cases be treated as equivalent to correspondence sent by traditional formal routes. Normal rules for authorising correspondence and statements should therefore be applied to electronic communication.

Access to the Internet by personal computers (including portables) provided by the Council must use only the approved service providers. (Downloading "free" browsers etc. may significantly change the way in which the PC is organised, which may in turn give rise to support problems.)

Users must not load unauthorised software, including games, on personal computers provided by the Council.

Users should print only essential material, and should check the length of a document before printing.

Use of the facilities provided will be routinely monitored and any unauthorised or unacceptable use could result in disciplinary measures.

Unacceptable Deliberate Use:

The following activities, whilst not an exhaustive list, are unacceptable:

1. The access to or creation, transmission or publication of any offensive, discriminatory, pornographic, obscene or indecent images, sounds, data or other material.

2. The access to or creation, transmission or publication of any data capable of being displayed or converted to such offensive, pornographic, obscene or indecent images, sounds, data or other material.

3. The creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety, or which may intimidate or create an atmosphere of harassment.

4. The creation, transmission or publication of defamatory material.

5. The receipt or transmission of material that infringes the copyright of another person.

6. The creation, transmission or publication of any material in violation of Data Protection legislation or of any UK or International laws or regulations. Such activity may constitute a criminal offence.

7. The transmission of unsolicited commercial or advertising material to other users of the Council's network or users of the Internet.

8. The deliberate unauthorised access to facilities, services, data or resources within the Council or any other network or service accessible via the Internet, or attempts to gain such access.

9. Personal use of the internet is only to be at lunch time and out of office hours working (i.e. when logged out on the daily timesheet

10. Unauthorised access to the electronic mail of another individual.

11. Deliberate activities with any of the following characteristics or that by their nature could result in:
    - wasting staff or other users' efforts or network resources
    - corrupting or destroying other users' data
    - violating the privacy of other users
    - disrupting the work of other users
    - using the internet in a way that denies service to other users (for example by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading large files)
    - continuing to use any item of software or to access any material after being requested to cease its use because of disruption caused to the functioning of the Council's network or the Internet (for example utilities designed to broadcast network-wide messages)
    - the introduction or propagation of viruses

12. Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network.

13. Any use of the Internet or other facilities that could damage the reputation of the Council.