CONGLETON TOWN COUNCIL

I.C.T. POLICY

Introduction

The Council uses its computer network, software packages and the internet, (including e-mails), to further the efficiency of its business and to provide the best service possible to its customers and partners. Any disruption to the use of these facilities will be detrimental to the Authority and may result in actual financial loss. This Policy sets out how the Council intends to regulate the use of those facilities.

The Council has a duty laid down in the Data Protection Act 1998, to ensure the proper security and privacy of its computer systems and data. All users have, to varying degrees, some responsibility for protecting these assets. Users also have a personal responsibility for ensuring that they and, where appropriate, the staff they supervise or have control over, comply fully with this policy – See also the Council's Information and Data Protection Policy.

For the purposes of this document the terms "computer" (or "computer system") and "computer data" are defined as follows:

"Computer" (or "computer system") means any device for automatic storing and processing of data and includes mainframe computer, minicomputer, microcomputer, personal computer(whether hand-held laptop, portable, standalone, network or attached to a mainframe computer), workstation, word processing system, desk top publishing system, office automation system, messaging system or any other similar device;

"Computer data" means any information stored and processed by computer and includes programs, text, geographic, pictures, video and sound.

General Operation

All hardware, software, data and associated documentation produced in connection with the work of the Council, are the legal property of the Council.

The Council will maintain an external support contract for the hardware, major items of software and provision of internet facilities.

The Council will not knowingly breach copyright of another person.

The Council will include an assessment of risks from its use of IT in its Business Risk assessment.

The Council will routinely back up its essential data and organise contingency plans.

The Council will make a detailed inventory of its ICT equipment on its Asset Register.

The Council will consider the location of equipment and provide documentation to ensure optimum physical security.

The Council will maintain a record of training to each individual user.

The disposal of any ICT equipment, software, waste or data must be authorised, undertaken safely and properly documented.

Compliance with Legislation

The Council's policy in respect of the requirements of the Data Protection Act 1998 is set out in its Information and Data Protection Policy.

Under the Computer Misuse Act 1990, the following are criminal offences, if undertaken intentionally.

- unauthorised access to a computer system or data;
- unauthorised access preparatory to another criminal action;
- unauthorised modification of a computer system or data;

All users should be made aware that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written "in-house", will be regarded as a breach of the Council policy and may be treated as gross misconduct. In some circumstances such a breach may also be a criminal offence.

It is an offence under the Copyright, Design and Patent Act to copy licensed software without the consent of the copyright owner. All copying is forbidden by the Act, unless it is in accordance with the terms and condition of the respective licence or contract.

Security

Consideration must be given to the secure location of equipment and documentation to help safeguard the Council's ICT assets. Portable equipment must be locked away when not in use and must not be removed from the premises without permission.

Only persons authorised by the Chief Officer may use Council computer systems. The authority given to use a system must be sufficient but not excessive and users must be notified that the authority given to them must not be exceeded.

Operating procedures are required to control use of ICT equipment.

Access to the Computers is subject to a password, which is periodically changed.

Virus Controls

Viruses are undesirable pieces of computer code that can corrupt systems, equipment and data. They are a serious, increasing threat to the computer systems of the Council.

All computer and servers will have loaded and operate the Council's standard virus detection software for scanning diskettes and fixed drives.

Diskettes of unknown origin should not be used in the Council's computers.

No software should be located onto the Council's equipment without the permission of the Chief Officer.

If a virus is suspected, the equipment should be switched off and isolated and the Council's support contractor should be contacted.

V5 10.05.18

Misuse

This Policy applies to the activities which constitute unacceptable use of the network operated by the Council. The policy applies equally to employees, councillors, clients, visitors and others who may be allowed to use the facilities on a permanent or temporary basis. All misuse of the facilities is prohibited including specifically but not exclusively the following:

1. The creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material.
2. The creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
3. The creation or transmission of defamatory material.
4. The transmission of material in any way that infringes the copyright of another person.
5. The transmission of unsolicited commercial advertising material to networks belonging to other organisations.
6. Deliberate actions or activities with any of the following characteristics:

- Wasting staff effort or networked resources
- Corrupting or destroying another users data
- Violating the privacy of other users
- Disrupting the work of other users
- Other misuse of networked resources by the deliberate introduction of viruses
- Playing games during working hours
- Private use of the facilities without specific consent
- Altering the set up or operating perimeters of any computer equipment without authority

World Wide Web (WWW) resources

These facilities are provided for use to achieve Council objectives. Any use for unauthorised purposes will be regarded as gross misconduct. If you are unsure whether use would be authorised, you must seek advice from the Chief Officer in advance.

Health and Safety

Computers are now a part of everyday life. If they are not used correctly, they can present hazards. Computers may be called Display Screen Equipment (DSE), Visual Display Units (VDU's) and the immediate environment where they are used i.e. desk/chair etc. is referred to as a workstation.

The Display Screen Equipment Regulations, 1992 regulate the use of computers at work and refer to the persons affected as "users".

"Users" are persons who "habitually use VDU's as a significant part of their normal work and regularly work on display screens for two/three hours each day or continuously for more than one hour spells". The Regulations also apply to employees working at home.

To meet the requirements of the Display Screen Equipment Regulations, the Council will provide a free eye test for all staff who use VDU equipment as a major part of their job role.

It is the Council's intention to optimise the use and application of display screen equipment within the Organisation, whilst safeguarding the health, welfare and job satisfaction or learning experience of those involved in using such equipment.

Staff "users" will have their name entered onto the list of "Designated Computer Users".

Risk assessments of all workstations are carried out to highlight any problems - this is done using the Workstation Assessment Questionnaire which is also a useful training tool.

If you are a "defined computer user":-

- Your workstation must be designed for computer use. There must be sufficient space to position your keyboard so that you can rest your wrists in front of it;

- The screen should be fully adjustable and must be positioned to avoid glare from lights, windows etc.;

- Your chair must be of the fully adjustable type with five castors and must be adjusted to support your lower back. It must be set at the correct height for your desk. Your feet should rest on the floor and you may need a footrest;

- Report eyestrain, headaches or aching limbs to your manager.

- Ensure your computer has an adjustable keyboard;

- Ensure your working environment is comfortable. Problems with ventilation, temperature or lighting should be reported to your Manager.

- Take a few minute break every hour

Appendix 1.

 PROTOCOL FOR USING CONGLETON TOWN COUNCIL'S WEBSITE (Feb 2013)

Background

The Town Council website was re-designed by Longton Company, Cyberzia Ltd; it went live in September 2011. The website is now hosted and supported by R1 Creative. The site www.congleton-tc.gov.uk is owned by the Town Council.

Updating the Site

The site will be updated on a daily basis or when required by Town Council staff. It is important that the site remains fresh, relevant and current. Should Councillors wish to have any content added or amended, please inform the Chief Officer.

Agendas will be uploaded onto the site at least 3 days prior to meeting dates; Minutes will be uploaded within 1 week of meeting dates.

Councillor details can be found on the 'Meet the Councillors' page of the site, personal contact details are listed with the permission of each Councillor. Also listed are any Appointments to Outside Bodies and any Declarations of Interests, if any changes need to be made the Chief Officer must be informed.

The Home page of the site has a 'twitter' feed which shows the 5 most recent 'tweets' sent from @Congleton Town, this can only be updated by the Town Centre & Marketing Manager and Town Council staff. Any 'tweets' sent out must be non-political, uncontroversial and used to promote/highlight events in the Town.

V5 10.05.18