Information & Communications Technology (ICT) Policy

1 Introduction

1.1 Sprowston Town Council will make the most of innovative new technology to make its services more efficient and accessible, particularly where the cost of change is outweighed by the benefits. Our ICT Policy has been produced to make clear how we will develop and control our computer systems.

1.2 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, partners and the public. Any disruption to the use of these facilities will be detrimental to the Council and may result in actual financial loss. This Policy sets out how the Council intends to regulate the use of these facilities.

1.3 The Council has a duty laid down in the Data Protection Act 1998, and in compliance with the General Data Protection Regulation ((EU) 2016/679) (GDPR) and the Data Protection Bill 2017 (DPB) 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 the staff they supervise comply with this policy – see also the Council's Information and Data Protection Policy.

1.4 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, tablet, 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.

2 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 off site.

- 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 securely and be properly documented.

- The Council will standardise where possible on Microsoft standard software.

- Maintain a Recovery Plan in case of loss, corruption or damage to ICT equipment, software or data.

3 Compliance with Legislation

The Council's policy in respect of the requirements of 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 conditions of the respective licence or contract.

4 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 Town Clerk may use Council computer systems. The authority given to use a system will be sufficient but not excessive and users will 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. Levels of encryption will be maintained according to risk.

Further development of appropriate secure data storage, off site back up of data, and recovery plans will be a priority for review.

5 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 computers and servers will have loaded and operate the Council's standard virus detection software including ransomware for scanning discs, memory sticks and fixed drives. Discs and memory sticks of unknown origin should not be used in the Council's computers.

No software should be loaded onto the Council's equipment without the permission of the Town Clerk.

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

6 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.

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 parameters of any computer equipment without authority

7 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 any member of staff is unsure whether use would be authorised, then permission in advance must be sought from the Town Clerk.

8 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.

It is important that a correct assessment of employees workstation is done to highlight any problems that must be reported to the Town Clerk – this is done using the Workstation Assessment Questionnaire. Completed questionnaires are returned to the Town Clerk.

If a person is a "defined computer user":-

- the workstation must be designed for computer use. There must be sufficient space to position the keyboard so that the operator can rest their wrists in front of it;
- the screen should be fully adjustable and must be positioned to avoid glare from lights, windows etc.
- the chair must be of the fully adjustable type with five castors and must be adjusted to support the lower back. It must be set at the correct height for the desk. The operators feet should rest on the floor and a footrest may be needed.
- eyestrain, headaches or aching limbs must be reported to the Town Clerk. The Council will pay for your eye test if you are a defined user;

- ensure the computer has an adjustable keyboard;
- ensure your working environment is comfortable. Problems with ventilation, temperature or lighting should be reported to the Town Clerk.

9 Protocol for the use of Sprowston Town Council's Website

The Town Council website was redesigned in 2013, it is managed in-house with information easily added or removed. The Town Clerk has editorial control. Quality is important to the image of the Council. It must be remembered that anything published on the web should be viewed the same as published in a local newspaper and needs to be accurate and in accordance with the Town Council Policy. The site will be updated at least weekly. It is important that the site remains fresh, relevant and current.

The Code of Recommended Practice on Local Authority Publicity – updated 2011 must be taken into account when matters of publicity are concerned, more details are provided in the Council's Communications & Marketing Policy. Basically the Council are allowed to publicise the contact details of individual councillors, positions they hold and can publicise individual proposals, decisions and recommendations but must keep information objective and not use Council funds to mount campaigns intended to persuade members of the public to hold a particular view on a question of policy or party politics.

Important links to make it easy for visitors to find out information about the Town and its organisations will be placed on the website. Other bodies will also be approached for them to have links to our site.

10 Social Media

A social network service focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others.

Most social network services are primarily web based and provide a collection of various ways for users to interact, such as chat, messaging, email, video, voice chat, file sharing, blogging, discussion groups. Social networks include, but not limited to Facebook, Twitter, LinkedIn, Bebo, My Space and personal blogs. This Council uses social media sites to publicise the Council's activities.

The staff handbook contains details of the standards employees are required to comply with, as follows:

- Employees will not maintain any site that contains personal identifiable information of the Council.
- Employees will not maintain a site that contains photographs of clients.
- Employees will not maintain a site that contains identifiable information of a client or an employee in relation to their performance and character.
- Employees will not maintain a site that contains photographs of another employee taken in the work situation.
- Employees will not maintain a site that contains defamatory statements about the Council, its current or ex-employees, the council's services or contractors.
- Employees must not express opinions on the sites that purport to represent their own views on the Council.

- Employees must never post a comment on the sites that purports to represent the views of the Council without first consulting the management team.
- Employees must not breach Council confidential information.

As an employee of the Council, the Council has a reasonable and lawful expectation that staff will not bring the Council into disrepute, this is extended to the home environment as well. Any grievance with the organisation should be processed through procedures and policies already in place and dealt with within the work environment.

If employees become aware of a breach in this policy they should contact their line manager in the first instance if it is appropriate to do so. It is possible such a matter may be resolved locally. If this is not the case and if staff are found to have contravened this policy disciplinary sanctions, up to and including dismissal can occur.

The Council reserves the right to access and monitor all emails and internet activities carried out on Council equipment including the use of any social networking site.

Sharing information with and between Councillors

Historically the office prints as necessary documents for councillors. The Council will in future need to review this, along with the possibility of more useable technology provision, Council specific email addresses and advice on the security of confidential information made available to councillors.