BINGLEY TOWN COUNCIL

Bingley Town Council, Myrtle Place, Bingley, BD16 2LF

Information Technology Security Policy

Introduction

The information the Council holds and the Information Technology (IT) systems and networks that support it are important business assets. Many potential threats to these exist, such as fraud, vandalism, virus infection, theft, loss, abuse of copyright, misuse of software and accidental damage. The International Standard: ISO 27001:2013 Code of Practice defines Information Security as the preservation of:

- Confidentiality: ensuring information is accessible only to those authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information by protecting against unauthorised modification; and
- Availability: ensuring information and services are available to authorised users when required.

The Council is committed to preserving the confidentiality, integrity and availability of our information assets:

- For sound decision making;
- To deliver quality services;
- To ensure data quality and accurate, up-to-date information;
- To comply with the law;
- To meet the expectations of our customers;
- To protect our customers, staff, contractors, partners and our reputation as a professional and trustworthy organisation;
- To ensure the Council can continue working without interruption; and
- To enable secure and appropriate sharing of information.

Scope

This Policy is mandatory and there are no exceptions to it. It applies to all employees of the Council, including temporary and contract staff (including agency staff), elected councillors, contractors, agents and partners, who have authorised access to the Council's IT systems. This Policy applies throughout the lifecycle of information held by the Council on all types of media, from its receipt or creation, storage and use, to disposal.

Policy Statement

The Council understands the importance of information security and privacy. It is increasingly dependent on IT systems and so the potential impact of any breach is also increasing. The Council must safeguard its information systems and ensure compliance with this Policy, to provide protection from the consequences of information loss, damage, misuse or prosecution.

The General Data Protection Regulation 2018 (GDPR) places a duty on the Council to demonstrate accountability and to have in place the organisational and technical measures to protect the personal data it holds and processes. Bingley Town Council is committed to providing

the levels of information security required to protect this data and this Policy helps to set out how the Council aims to achieve the necessary standards. We also aim to fulfil the business needs of the Council and to allow staff to work in a flexible way, whilst maintaining the security levels required.

Legal and Regulatory Requirements

The Council has an obligation to ensure all its information systems and information assets and users of those systems and information assets comply with the following:

- Civil Contingencies Act 2004;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988;
- Data Protection Act 1998/2018;
- Electronic Communications Act 2000;
- General Data Protection Regulation;
- Payment Card Industry Data Security Standard;
- Privacy and Electronic Communications Regulations 2003 and E? Privacy Regulation 2018;
- Public Services Network Compliance; and
- Telecommunications (Lawful Business Practice) Regulations 2000.

If you are unsure about the relevant legal or regulatory requirements relating to the information you use in your work, please contact the Town Clerk for guidance.

Controls

The Council has information security measures in place to help mitigate risk, known as controls. These controls are divided into three categories: administrative, technical and physical.

Administrative Controls

A written Information Technology Security Policy document (this document) is available to all. Users are required to read this Policy.

All authorised users of the Council's IT equipment and systems have responsibilities to protect information assets and comply with information security procedures. However, the Town Clerk has overall accountability and responsibility for understanding and addressing information risk, including within their own service areas and for assigning ownership for information assets to others. Information assets held by the Town Council are follows:

- Allotments data base
- Rialtus data base
- E-mail lists
- Mail Chimp
- Drop Box

Technical Controls

Technical Controls are addressed within this policy and comprise the IT network and its software protection programmes.

Physical Controls

Physical Controls are addressed within this policy and comprise the human behaviours and disciplines put in place by our IT users to provide protection.

Network Security

Bingley Town Council does not operate an IT network. The Council's IT infrastructure therefore consists only of Council owned laptops, phones and printers.

The Council accesses all services required via the internet and the World Wide Web. As such the biggest risk to our IT security is incoming viruses from the World Wide Web. Mitigation of this risk is covered in this Policy.

Security of passwords is essential. Each user is responsible for the security of their passwords:

- Do not let anyone else know your passwords. Change passwords regularly and choose a password that is hard for others to guess.
- Do not leave a computer that is logged into the network unattended without first locking your screen.

All PCs owned by the Council will be equipped with suitable antivirus software to protect the Council from computer virus infections and other harmful programs:

- If you suspect the equipment you are using may be infected, switch off and disconnect from the network. When this is done, report to the Town Clerk as soon as possible.
- Email itself is rarely harmful; it is primarily documents or programs attached to an email that can contain viruses. If you do not recognise the sender, or have any doubts at all about an email, do not open it; it is better to delete it. Never open attachments or click on links within an email unless you are certain you know where the email has come from.
- Websites are another source of viruses. The Council's anti-virus software will automatically detect any viruses before anything is downloaded. If you see a warning message, leave the website and contact the Town Clerk.

Be vigilant when browsing the internet and accessing web-based personal email systems using corporate equipment. If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing it to be transmitted. So always take care, do not open anything suspicious and, if in any doubt, contact the Town Clerk.

Removable Media Controls

Assets are things of value. The Council has few IT assets but this Policy aims to protect those related to the Council's network. The Town Clerk is responsible for maintaining a database of all IT assets. IT assets are allocated to an individual, who has use of and is responsible for them.

- Laptops themselves are a form of remote storage and will be protected with suitable antivirus software,
- All remote storage devices such as memory sticks will be swept by antivirus software before use.

Secure Configuration

The Council's computers are to be set to 'automatic updates' to ensure that they are properly patched with the latest appropriate updates, to reduce system vulnerability and enhance and repair application functionality. Appropriate information backup is to be maintained, back up should be automatic and not left to user actions. Back up should ideally be automatic. Care needs to be taken that non automised back is carried out each month. Back up hard drives should be stored in a fire proof box.

User Education & Awareness

All authorised users must receive appropriate training, including information security requirements. It is the responsibility of the line manager to ensure that staff undertake the training provided. All new employees are made aware of this Policy as part of their induction.

The Council's IT equipment and systems may only be used for the conduct of personal purposes in line with the Town Council Communications and Social Media policy. Under no circumstances can Council IT systems be used for private commercial activity. Failure to comply may result in disciplinary action for staff or councillors being reported to the Monitoring Officer for councillors.

Malware Prevention

Do not copy licensed software, install or use unlicensed software. Software is protected by copyright.

Do not download material such as fonts, drivers, shareware or freeware without proper authorisation from the Town Clerk.

Do not copy or download material or publish it on the Council's website, unless you have permission to do so. Much of the material on the internet is protected by copyright. The Council retains copyright and intellectual property rights over material produced.

If the presence of 'malware' is suspected then a proprietary brand of malware detection, i.e. Malwarebytes, can be downloaded and run. NB. Do not subscribe to Malwarebytes as this is treated as an unauthorised purchase. Malwarebytes is available free of charge.

Home & Mobile Working

Staff and Members who use portable corporate devices, such as laptops, iPads & tablets and mobile phones must be particularly vigilant, since these devices are more likely to be lost, damaged or stolen.

Authorised working from remote locations such as home or conferences is permitted. Care must be taken when using Council IT infrastructure away from the office to ensure that laptops and phones are:

- not left unattended in a public place,
- not left in view in unattended vehicles,
- not be taken abroad, unless permission is approved by the Town Clerk.

Incident Management

All security incidents must be reported immediately to the Town Clerk. All authorised users have a responsibility to promptly report any suspected or observed incident.

Incidents that result from deliberate or negligent disregard of any security policy requirements may result in disciplinary action being taken. All incidents will be captured, recorded and reviewed, so that they can be effectively managed and lessons learned.

Managing User Privileges

The Town Clerk will maintain a record of users of Council owned IT infrastructure. Records will be kept of users of external systems and services, such as banking systems, Parish Online, etc, used by employees and Councillors. User privileges will be maintained by operators of such external systems and services.

Monitoring

The implementation of this Policy will be monitored to ensure compliance. An audit of software and hardware will be conducted on a regular basis.

• Any breach of this Policy by staff may lead to disciplinary action.

• Any breach of this Policy by a Councillor may lead to a complaint to the Monitoring Officer.

All equipment eventually becomes unusable, or no longer fit for purpose. It is vital to ensure that all data is destroyed to the appropriate level before any equipment is disposed of. Where an approved recycling organisation is used to dispose of the equipment, they must provide a certificate of destruction. All redundant Council IT equipment must be handed back to the Town Clerk so that it can be disposed of correctly.

Review

This Information Technology Security Policy will be reviewed annually and updated as required.

Adopted by the Council: 28th April 2020

Date of review:

Next review: