Adopted at Finance & Delivery Committee – 01/09/2025

Information Security Policy

1. Introduction

1.1 This policy has been adopted by the Town Council ("Council") in order to:

- Prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material).
- Protect confidential, personal or commercially sensitive data.
- Prevent the introduction of viruses.
- Prevent the use of unlicensed software.
- Ensure the Council property is properly looked after.
- Monitor the use of computer facilities to ensure compliance with internal policies and rules and to detect abuse.

1.2 The consequences of misuse can be severe. Examples of potential damage include, but are not limited to, malware infections, legal and financial penalties for data leakage and lost productivity from network downtime.

1.3 The Council provides Councillors and employees with access to various computing and telephone communication methods ("facilities") to allow them to undertake the responsibilities of their position and to improve internal and external communication.

2. Scope

2.1 This policy sets out the Council's position on the use of the facilities and it includes:

- Employees and councillors' responsibilities and potential liability when using the facilities.
- The monitoring policies adopted by the Council; and guidance on how to use the facilities.

2.2 This policy has been created to:

- Ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring.

- Protect the Council from the risk of financial loss, loss of reputation or libel; and

- Ensure that the facilities are not used so as to cause harm or damage to any person or organisation.

3. Breach of Policy

3.1 In respect of employees, breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's disciplinary process.

3.2 Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal grievance procedure.

4. Compliance with related Policies and Agreements

4.1 The Council's policies and procedures (e.g. Code of Conduct, Disciplinary, Data Protection and Equality & Diversity Policy) apply equally to behaviour online as well as off-line. The IT resources should never be used in a way that breaches any of our other policies.

4.2 It is your responsibility to ensure that information and data that you hold on the Council's computer systems complies fully with the principles of the General Data Protection Regulation (GDPR). In brief, the GDPR requires that anyone who inputs, stores or uses personal information must ensure that the information (e.g. names, addresses, other information kept on individuals) is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Processed in a manner that ensures appropriate security of the personal data.

- A good way of understanding these requirements and your responsibilities is to think about how you would wish your bank to store and use and not use, your own personal details. Please refer to our Data Protection Policy.

5. Email (Internal or External Use)

5.1 All Councillors and relevant employees will be issued with a Council email account which must always be used when transacting on behalf of the Town Council. Such account will only be used for Council correspondence.

5.2 Email should be treated as any other documentation. If you would normally retain a certain document in hard copy, you should retain the email.

5.3 As with any other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

5.4 Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of an email is strictly prohibited.

5.5 Take care that emails will be seen only by the person intended. Particular care should be taken when sending confidential information that the email has been correctly addressed, marked 'private' and not copied in to those not authorised to see the information. Sending confidential information via email without proper authorisation or without taking sufficient care to ensure that it is properly protected will be treated as misconduct.

5.6 While a reasonable amount of personal use of email is perfectly acceptable, your email remains the property of the Council and you should not use your Council email to send or receive any information that you regard as private. The Council may, in the course of its operation, read emails that you have sent or received - although in the absence of evidence of wrongdoing the Council will try to avoid reading personal emails if possible.

5.7 Councillors and employees will be required to surrender their email account and all of its contents to the Town Clerk when they leave the Council. The Clerk on leaving the Council needs to the same, but the Leader of the Town Council.

6. Laptop computers, PC's, tablets and mobile phones

6.1 Laptop computers, PC's, tablets and mobile phones belonging to the Council along with related equipment and software are subject to all the Council's policies and guidelines governing non-portable computers and software.

6.2 When using such equipment:-

- You are responsible for all equipment and software until you return it. It must be kept secure at all times.

- The Town Clerk and the individual employees or Councillor are the only persons authorised to use the equipment and software issues to that employee or Councillor.

- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention, initially through the Town Clerk, or in their absence the Deputy Clerk.

- Upon the request of the Council at any time, for any reason, you will immediately return any equipment and all software to the Council.

- Software piracy could expose both eh Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licenses to which the Council is a contracting party. This means, that:

    - Software must not be installed onto any of the Council's computers unless this has been approved in advance by our IT Contractors or the Council. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer facilities.

    - Software should not be removed from any computer, nor should it be copied or loaded on to any computer without prior consent.

7. Internet

7.1 Internet connection is for business purposes only. The only exception is for personal use during normal working hours in the Officer's own time.

7.2 Employees with access to the internet on Council-owned devices should use that access responsibly. Excessive personal use during working hours will be treated as misconduct. From time to time the Council may block access to sites which it considers inappropriate but whether or not a specific site has been blocked, employees must not use the internet to view or download offensive or sexually explicit material. Any attempt to do so may, depending on the circumstances, amount to gross misconduct leading to dismissal.

7.3 The downloading of files, shareware or freeware to the Town Council's processors is authorised for business use only and is considered a high risk activity. Any applicable licence conditions must be complied with. The

downloading of games, screensavers and other "fun" software is not considered to be legitimate business activity. These are more likely to contain viruses and programming errors which can severely compromise the Town Council's systems.

7.4 Firewalls and anti-virus software may be used to protect the Council's systems. These must not be disabled or switched off without the express authorisation of the Town Clerk.

8. Social Media

8.1 The Council may use social media to communicate messages to residents and will only be used:

- By the Town Clerk and persons authorised by the Town Clerk.
- To transmit factual information and news, not personal opinion.
- To respond to comments and requests submitted via the account.

8.2 Employees and Councillors using their own social media accounts must ensure that any comment made is clearly identified as their own and not representative of the Council.

8.3 An employee's behaviour on any social networking or other internet site must be consistent with the behaviour required of employees generally. Where it is possible for users of a social media site to ascertain who you work for, then you should take particular care not to behave in a way which reflects badly on the Council. Inappropriate or disparaging comments about the Council, colleagues or the town will be treated as misconduct. Because social media interactions can be copied and widely disseminated in a way that you may not be able to control, the Council will take a particularly serious view of any misconduct that occurs through the use of social media.

9. General Guidance

9.1 Observation of this policy is mandatory and forms part of the terms and conditions of employment of employees and the terms of access to the Council's systems and offices. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

9.2 You must ensure that portable computers and any other easily stolen equipment is securely locked away when not in use.

9.3 If you leave your terminal or PC unattended for up to 10 minutes, a password-protected time out or screen saver must be operating.

9.4 Monitoring of email usage takes place without notice. You should have no expectation of privacy in respect of personal and business use of email and the internet whilst at work.

9.5 Unauthorised access to any of the Council's systems will amount to gross misconduct.