Information Technology Policy

Responsibility: Personnel committee

Review Cycle: Every three years, or earlier in the event of legislative changes

Date of Adoption / Renewal	Resolution Number
6 December 2011	6347
16 December 2013	7043
21 February 2017	7996
2 February 2021	9250
7 April 2021	9331
26 March 2024	10469

INFORMATION TECHNOLOGY POLICY

1. Introduction

1.1 The purpose of this policy is to ensure that all employees and councillors using Crowborough Town Council information technology and systems have an understanding of what is and is not permitted. This will ensure the appropriate use of the council's equipment, safeguard the security of its IT systems and data, and assist compliance with Data Protection law.

2 Internet usage

Access to the council's IT systems is controlled by the use of user IDs and passwords. All User IDs and passwords are uniquely assigned to named individuals and consequently individuals are accountable for any action undertaken using their unique login details.

2.1 Individuals must not:

- Leave their user accounts logged in and unattended
- Leave their password unprotected or accessible to others
- Perform any unauthorised changes to the IT systems or information
- Attempt to access data that they are not authorised to use or access

2.2 Staff members must use the internet responsibly as part of their official and professional activities.

2.3 Information obtained via the internet and published in the name of the council must be relevant and professional. A disclaimer must be stated where personal views are expressed. Staff members should refer to the council's social media policy for information specific to sharing content via social media channels.

2.4 The use of the internet to access and/or distribute any kind of offensive or illegal material will not be tolerated and staff may be subject to disciplinary action.

2.5 The equipment, services and technology used to access the internet are the property of the council. The council reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

3 Unacceptable use of the internet

3.1 Unacceptable use of the internet by staff members includes, but is not limited to:

- sending or posting discriminatory, harassing or threatening messages or images
- using computers to perpetrate any form of fraud, and/or software, film or music piracy
- obtaining, using or disclosing another staff member's password without authorisation
- sharing confidential material or proprietary information outside of the council
- hacking into websites

- sending or posting information that is defamatory to the council, its services, councillors and/or members of the public
- introducing malicious software onto council computers and/or jeopardising the security of the council's electronic communication systems
- sending or posting chain letters, solicitations or advertisements not related to council business or activities
- passing off personal views as those representing the council
- accessing inappropriate internet sites, web pages or chat rooms

3.2 If a staff member is unsure about what constitutes acceptable internet usage, they should approach their line manager for further guidance and clarification

4. Email

4.1 Email should be regarded as written paper documents for the purposes of production, use, retention and disclosure and can be called upon under the Freedom of Information Act 2000. Personal information should be kept in accordance with the principles established in the Data Protection Act 2018 and General Data Protection Regulation.

4.2 The council reserves the right to open any email file stored on the council's computer system.

4.3 The following guidelines for email use should be observed by all staff members and councillors:

- use appropriate language to avoid unintentional misunderstandings
- respect the confidentiality of information contained within emails, even if encountered inadvertently
- check with the sender if there is any doubt regarding the authenticity of a message
- do not open any attachment unless certain of the authenticity of the sender
- only copy emails to others where appropriate and necessary
- emails which create obligations or give instructions on behalf of the council may only be sent by officers
- emails must comply with common codes of courtesy, decency and privacy

4.4 Emails should not be kept longer than they are required in line with the Data Protection Act 2018 and GDPR UK.

Article 5 (1) e
Personal data shall be:
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; personal data may be stored for longer periods in sofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this regulation in order to safeguard the rights and freedoms of the data subject (storage limitation)

5. Security

5.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5.2 In the event of personal data breach consideration must be taken into account as to whether this poses a risk to people's rights and freedoms, following the breach. A personal data breach must be reported to the Town Clerk who will make an assessment of the breach and whether to report the breach to the ICO.

5.3 All council equipment and data, for example laptops and mobile devices, must be returned to the council at termination of contract or at the end of the tenure in the case of councillors.

5.4 All council data or intellectual property developed or gained during the period of employment remains the property of the council and must not be retained beyond termination or reused for any other purpose.

5.5 Only software purchased by the council shall be installed on the council's computer system. Software licences shall be retained.

6. Reporting and sanctions

6.1 If a councillor receives an email which is considered to be in breach of this policy, it should be referred to the Town Clerk for investigation. This investigation may result in the use of the formal disciplinary procedure.

6.2 If a staff member receives an email from a councillor which is considered to be in breach of this policy it should be referred to the Town Clerk for investigation. The staff member is entitled to consider use of the council's grievance policy and/or report the issue through the procedures outlined in the Member's Code of Conduct.