

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

1. What is Information and Communication Technology?

Information and Communication Technology (ICT) is a loose term which is used to describe a wide range of tools and techniques, usually electronic in nature, which speed up and/or aid communication.

Keynsham Town Council recognises the importance of embracing ICT in order to ensure that its customers benefit from efficient delivery levels of service.

The Council supports the Government's aim of improving electronic access to public services.

2. Aims

The aims of this policy are to:

- i) facilitate the ongoing development of the efficient management and delivery of the Council's services;
- ii) provide opportunities for staff to acquire and develop core ICT competencies;

3. Scope

This policy applies to all **councillors, employees, volunteers, and contractors** who use or manage the council's IT resources, including but not limited to:

- Desktop and laptop computers, tablets, and smartphones
- Email and cloud-based systems
- Council website, social media, and digital publication tools
- Video conferencing and messaging platforms
- Personal devices used under Bring Your Own Device (BYOD) provisions

4. Governance and Oversight

IT Oversight: The Clerk is the designated Data Protection Officer (DPO) and IT Systems Administrator.

5. Data Protection & Security

All processing of personal data shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Privacy Policy: All data collection, processing, and subject rights are governed by the council's Privacy Policy, available on the council website.

Access and Storage: Data is stored securely, with access granted only to authorised personnel based on necessity.

Retention: Personal data will be retained in accordance with the council's Data

Retention Schedule and securely deleted when no longer needed. See Data Retention Policy.

6. Technical Support

The Town Council shall appoint an independent and competent ICT support provider (currently SoVision IT Ltd, Keynsham) and will be subject to a 3-year review in order to confirm the service they provide to meet delivery needs.

7. Security

a) Individuals (Staff and elected Members) shall:

- be responsible for the Town Council's usernames and passwords;
- Strong password protection with multi-factor authentication where possible is required for all systems.
- Passwords used on council systems are to be unique to this environment and no user in scope must use logins associated with non-council systems.
- protect user credentials against misuse;
- not share or disseminate any user credentials with another person; only attempt to access ICT where permissions have been given; not misuse or alter the configuration or settings of any ICT;
- not attempt to bypass or subvert ICT security controls; not leave a computer system open if it is unattended;
- operate a clear screen policy when you leave ICT unattended, for example by temporary "locking" the computer;
- Regular security updates and anti-malware software are required on all council-owned and personal devices.
- Backups of essential data must be stored in a secure location.
- All Council-owned ICT portable media and devices shall be protected at all times, in particular when transporting them outside of Council premises. Where appropriate items should be secured within the fireproof storage within the Town Council offices;

b) All ICT media and portable devices used to process any Council information shall be password protected and encrypted.

c) Staff will seek to prevent inadvertent disclosure of personal or sensitive information by avoiding being overlooked when working

d) Staff and elected Members shall take care when both printing or disseminating information and will carefully check any distribution list before any material is to be transmitted.

e) Staff and elected Members shall securely store or destroy any printed material which contains private information, sensitive, disclosive or identifiable records including personal data or material which is not for public circulation.

f) Staff and elected Members shall not introduce unofficial software, hardware, removable media or files without appropriate authorisation.

g) Staff and elected Members shall report any security incident or suspected security incident to the Council as soon as is reasonably possible.

8. Hardware

Computers and peripherals

The Town Council's computer systems and computer peripherals will be subject to annual review in order to confirm that they are meeting service delivery needs.

The current printer/scanner/copier is leased from Xerox with monthly charges from ITEC.

All computers and computer peripherals will be listed, and revisions / deletions will be assessed for replacement or upgrade over a maximum of a 3-year period.

9. Telephones and related systems

The Town Council currently utilises the telephone system supplied by Microtalk within the office leasing agreement; this practice will be subject to three-yearly review.

Facsimile and / or answer machines (or such combined units, where supplied) will be maintained within the Town Council office. Any information contained in outgoing messages (conveyed by the latter machine) will conform to national minimum standards with messages being clear and concise.

Except for exceptional circumstances, use of the telephone, related and electronic communication systems for personal use must be authorised by the Town Clerk.

There is no foreseeable requirement to issue all staff with mobile phones other than the Grounds Maintenance Staff, Cemetery Attendant and the Youth Staff. There is a mobile phone utilised by office staff for the purpose of keeping in touch with the Cemetery Attendant as part of Lone Working provision and the Town Clerk will need a mobile phone to receive security codes/passwords to access HMRC, Pension, Banking and other websites as their security and log in protocols are increased..

All telephone and related systems will be assessed over a 5-year period and assessed for replacement/repair where necessary.

10. Audio-visual Equipment

The projector equipment is and remains the property of Keynsham Town Council. The service and repair of such equipment is the responsibility of Keynsham Town Council.

Any equipment service or breakdown issues must be reported to the Town Clerk at the earliest opportunity.

11. Software

The Town Council's computer software will be subject to annual review in order to confirm

that it is meeting service delivery needs and demand.

In order to ensure adequate maintenance and development support, the Council shall normally avoid bespoke software packages. The Town Council currently licensing Office 365 accounts for all users.

- The Town Council approved applications are word processing:
- Microsoft Word Microsoft Excel spreadsheets: Microsoft PowerPoint presentations: Microsoft Publisher and Full Adobe Creative Cloud for Marketing & Communications Assistant publications:
- email: Microsoft Outlook
- shareware – Microsoft one-note, drop box or one-drive
- pensions: i-Connect
- accounting: RBS (bespoke package)

12. Internet access

The Town Council recognises that the Internet is a valuable information resource with the potential to improve the delivery of its services.

Access to the Internet for 'leisure' purposes is permitted during authorised break times. Access for personal reasons is permitted in certain circumstances, however it is the responsibility of the 'user' to ensure no illegal or prohibited sites are accessed; should this happen by error a report should be immediately submitted to the Town Clerk / Chairman of the Council.

13. E-mail

The Council recognises that email is an increasingly popular, speedy and cost-effective method for communication and data transfer.

The Council requires that the Town Council office in Temple Street Keynsham has the capability of sending/receiving email messages and data. There is also a WIFI requirement for both staff and members of the public. Members of staff will have their own secure wireless access which will connect with the Council's server. Members of the public will have a secure Wi-Fi connection to the internet.

Members of staff and authorised users shall ensure:

- e-mail use must be lawful and inoffensive - and be approved by an authorised user, normally the Town Clerk;
- they do not send personal or sensitive data over public networks such as the Internet unless an approved method of protection or encryption has been applied to it;
- they check that the recipients of e-mail messages are correct so that personal, or sensitive information is not accidentally released into the public domain;
- that personally owned email accounts are not used to conduct Council business;
- personal use of the Internet shall be reasonable, proportionate and occasional and shall not interfere with the performance of your role or the performance of the system;

- they do not use Town Council e-mail address(es) to send personal emails unless the item
- is marked as 'personal' and the sender clearly identifies that such communication.

14. Unacceptable Use

Members of staff and authorised users shall ensure:

- any security incident or suspected security incident to the Council as soon as is reasonably possible;
- they do not send personal or sensitive data over public networks such as the Internet unless an approved method of protection or encryption has been applied to it;
- they check that the recipients of e-mail messages are correct so that personal, or sensitive information is not accidentally released into the public domain;
- they do not communicate information via an ICT system knowing it or suspecting it to be unacceptable within the context and purpose for which it is being communicated;
- they do not process or access racist, sexist, defamatory, offensive, illegal or otherwise inappropriate material;
- they do not carry out illegal, fraudulent or malicious activities;
- they do not store, process or display offensive or obscene material, such as pornography or hate literature;
- They do not annoy or harass another individual, for instance by sending chain letters, uninvited e-mail of a personal nature or by using lewd or offensive language;
- they do not break copyright;

15. Use of Personal Email Addresses

Prohibited Practice: The use of personal email accounts for council business is strictly prohibited. All council correspondence must be conducted through official council-provided email addresses. Council emails must not be shared or forwarded outside of approved data areas, such as forwarding to a non-council-owned domain or personal email.

Monitoring and Compliance: Any breaches will be investigated, and appropriate measures taken in line with the council's disciplinary or governance procedures.

Email Retention: All council emails will be stored in compliance with the GDPR, DPA and Freedom of Information requirements.

Correspondence protocol – all councillors using council-owned email systems will ensure the clerk is copied into all correspondence, including replies.

16. Remote Access

The Town Council recognises that staff may need to work from remote locations from time to time. To address this issue, provision for remote access is available. Log on and password information will be issued to staff members. Staff members shall report any security incident or suspected security incident to the Town Clerk and the Council as soon as is reasonably possible.

17. Access Control

Should any personnel or member leave the Council, the Clerk (or instructed council officer) will rescind access to all Council systems for the person leaving. This includes changing the password and freezing the email account(s), access to council systems (accounting software, cloud storage, website admin) and handing back the Council's tablet to the Clerk.

Even though the policy states no personal email account is to be used, any personnel or member who leaves the Council must delete any Council emails on their personal email accounts in their procession.

18. Personal Data

Any member of staff processing personal data must comply with the eight enforceable principles of good practice (Data Protection Act 1988 & 2018).

These stipulate that data must be:

- i) used fairly, lawfully and transparently
- ii) used for specified, explicit purposes
- iii) used in a way that is adequate, relevant and limited to only what is necessary
- iv) accurate and, where necessary, kept up to date
- v) kept for no longer than is necessary
- vi) handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

19. Data Protection

i) Confidentiality

Passwords are to be used to restrict access to personal and/or confidential data. If there is any doubt about whether access to certain data should be restricted, guidance should be sought from the Town Clerk.

ii) Viruses

All computers used to send/receive emails or to access the Internet must have recognised anti-virus software installed - such as Avast, Norton Anti-Virus or McAfee.

No disk, drive or memory stick from any external source shall be opened until it has been checked for viruses.

20. Training

The Council recognises that training staff using new technology products is essential.

Therefore:

- i) all users of IT office productivity facilities (such as word processing and spreadsheets) shall be given appropriate training;
- ii) adequate training in the use of specialised or bespoke software packages will be given to all users of that software;
- iii) training will be given to users of any new software as part of the implementation program.

21. Awareness

Individuals shall make themselves aware of, and comply with, requirements and legislation

regarding information security and data protection along with any other legal, statutory or contractual obligations identified by the Town Council.

22. Monitoring

The Town Council reserves the right to monitor or record all communication systems including email, electronic messaging and internet use. Records of activity may be used by the organisation for the following purposes

- quality assurance

- conduct

- discipline

- performance

capability and/or criminal proceedings and any other purpose compliant with the regulatory and legislation framework in force and useful to support the Council's business activities.

23. Breaches of Policy

All Council employees have a contractual responsibility to be aware of and conform to the Council's values, rules, policies and procedures. Breaches of policy may lead to disciplinary proceedings.

Individuals who fail to comply with the Council's policies and who are not Council employees may have their access to Council information and ICT revoked and such action could have impacts on contracts with third party organisations.

24. Data Breach Process and Protocols

The Town Council is committed to responding promptly and effectively to any data breaches to minimise risk and comply with UK GDPR and DPA requirements.

24.1 Definition of a Data Breach

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising council systems

24.2 Reporting a Breach

Immediate Notification: Any councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Clerk (Data Protection Officer).

Initial Response: The Clerk in consultation with Council will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling 2FA).

24.3 Investigation

A full investigation will be conducted by the Clerk or designated officer within 72 hours

of the breach being discovered.

The breach will be logged, including:

- Date and time of breach
- Type and volume of data affected
- Cause and extent of the breach
- Actions taken to address the breach

24.4 Notification Requirements

If the breach is likely to result in a risk to the rights and freedoms of individuals, the council must notify the Information Commissioner's Office (ICO) within 72 hours.

* If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay, outlining:

- The nature of the breach
- Likely consequences
- Measures taken to mitigate the risk
- Contact information for further support

Signed (Chair of Town Council):

A handwritten signature in black ink, appearing to be "A. Jones", written over a dotted line.

Date: 15 09 26

Signed (Town Clerk):

A handwritten signature in black ink, appearing to be "D. Jones", written over a dotted line.

Date: 15th September 2026