CREDITON
TOWN COUNCIL

Manor Office
6 North Street
Crediton
Devon
EX17 2BR
Telephone: 01363 773717
Email: reception@crediton.gov.uk

IT and Data Protection Policy

Introduction

This policy sets out the responsibilities of all elected and co-opted members of Crediton Town Council (CTC) in relation to their use of IT systems, handling of personal data, and compliance with data protection legislation.

It sits under and supports CTC's Information & Data Protection Policy and ensures members meet the requirements of UK GDPR, the Data Protection Act 2018, and Audit Assertion 10 obligations.

Scope

This policy applies to all members when carrying out their duties, including:

- Use of council-provided email addresses and IT systems
- Handling of personal data of residents, staff, contractors, or partners
- Storage, sharing, and deletion of council-related information on personal or council devices.

Key Principles

Use of Council Email & Domain

- Members must use their council-owned email address for all CTC business
- Personal email accounts (e.g. Gmail, Hotmail) must not be used for CTC business
- Members must not set up auto-forwarding of CTC emails to personal accounts.

Use of Devices

- Council-owned devices should be used for CTC business
- All members receive a council-owned device, and are required to sign for the device and abide to the rules of their use
- If personal devices (laptops, tablets, smartphones) are used, they must:
    - Be password-protected or secured with biometrics
    - Have up-to-date antivirus protection
    - Be locked when unattended
- Members must always log out of all CTC accounts when not in use.

Handling of Personal Data

- Members must treat all personal data received in their role as confidential.
- Personal data must not be downloaded or stored permanently on personal devices.
- If temporary access is required (e.g. opening an email attachment), it must be deleted as soon as no longer required.
- Hard copies of personal data must be stored securely and destroyed via shredding or by using CTC's confidential waste system.

Data Sharing

- Personal data must only be shared where it is lawful and necessary for CTC business.
- Data must not be shared informally (e.g. WhatsApp, Messenger, personal social media).
- Any request for information should be referred to the Town Clerk for advice.

Data Retention and Deletion

- Members must ensure personal data is not kept longer than necessary.
- Emails and documents containing personal data must be deleted when no longer required for CTC business.
- On leaving office, members must ensure all council-related data is handed back to the Town Clerk and removed from personal devices.

Security & Breach Reporting

- Any loss, theft, or suspected breach of council-related data (digital or paper) must be reported to the Town Clerk immediately.
- Members must co-operate fully with the Town Clerk in investigating and addressing any breach.

Confidential Papers Issued for Meetings

- All confidential papers issued for meetings are issued as part of members' agenda packs, but are not published in the public agenda pack.
- All confidential papers must not be shared or discussed outside of the covened meeting.
- At the end of the meeting, any printed papers should be handed to the Town Clerk of the meeting for secure disposal.

Training and Compliance

- Members must undertake basic GDPR and data protection training at least once per term of office.
- All members must confirm in writing that they have read, understood, and will comply with this policy.
- The Information Commissioner's Office https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/ has a number of useful modules providing guidance on topics such as:
    - data protection principles
    - security (data protection and cyber)
    - online security and data protection
    - what is personal information.

Enforcement

Failure to comply with this policy may result in:

- Referral to the Monitoring Officer for a potential breach of the Code of Conduct
- Referral to the Information Commissioner's Office if a serious data protection breach occurs.

Name:……

I confirm that I have read and understood the contents of this policy and agree to adhere to its contents.

Signed:……..

Date:……..