**Croxdale and Hett Parish Council**

**IT Policy**

## 1. Purpose

This policy outlines the principles and procedures for the use, management and security of IT systems, devices, and data within Croxdale and Hett Parish Council. It aims to ensure that technology is used responsibly, securely and in compliance with legal and regulatory requirements.

## 2. Scope

This policy applies to:

- All Parish Council members and employees
- All devices, software and digital services used for Council business

## 3. IT Governance

- The Clerk is responsible for day-to-day IT management and liaising with external IT providers.
- The Council will ensure appropriate budget provision for IT maintenance, upgrades and cybersecurity.
- All IT purchases must be approved by the Council and comply with procurement procedures.

## 4. IT Policy

**Parish Clerk**:

- The Parish Clerk will be assigned a Council email address for official correspondence.
- The Parish Clerk is responsible for safeguarding any Council devices, data, or systems under their control.

**Members:**

- Members will be issued Council email addresses for all Council-related communications.
- Emails relating to Council business are considered Council data and may be subject to disclosure under the Data Protection Act or Freedom of Information Act, even when sent from personal accounts.
- Incoming emails to member accounts are stored on the server per the Data Protection Policy.
- Personal devices used to access Council systems must be password-protected and accessible only by the member.

## 5. Acceptable Use

- Council IT systems and devices must be used only for official Council business.
- Personal use of Council devices (if applicable) is discouraged and must not compromise security or data integrity.
- Users must not install unauthorised software or access inappropriate content.

## 6. Data Protection and Privacy

- All personal data must be handled in accordance with the UK GDPR and Data Protection Act 2018.

- The Clerk is the designated Data Protection Officer (DPO) and responsible for ensuring compliance.
- Personal data must be stored securely and only accessed by authorised personnel.
- Data breaches must be reported immediately to the Clerk and documented.

**7. Email and Communication**

- Council email accounts (e.g. @croxdaleandhett-pc.gov.uk) must be used for all official correspondence.
- Councillors are encouraged not to use personal email accounts for Council business.

**8. Website and Social Media**

- The Clerk is responsible for maintaining the Council website and ensuring content is accurate and up to date.
- Social media posts must reflect Council decisions and policies.

**9. Security and Access Control**

- Devices must be password-protected and updated regularly.
- Access to sensitive data and systems must be restricted to authorised users.
- Remote access must be secured via VPN or encrypted connections.
- Anti-virus and firewall protection must be maintained on all Council devices.

**10. Equipment and Asset Care**

- Council devices and equipment must be handled responsibly and securely.
- Loss or damage of equipment must be reported immediately to the Clerk or Full Council.
- Council-owned devices remain the property of the Council and must be returned promptly if an individual leaves their role.
- Council computer equipment (laptop) is provided for Council purposes or a personal laptop can be used, subject to agreement by the Parish Council.

**11. Backups and Disaster Recovery**

- Regular backups of Council data must be performed and stored securely.
- The Parish Council's risk assessment should be referred to ensure continuity of operations in the event of IT failure or data loss.

**12. Reporting and Enforcement**

- Any IT issues, security concerns, or suspected breaches must be reported to the Clerk immediately.

**13. Review and Updates**

This policy will be reviewed annually or sooner if required due to changes in legislation, technology, or Council operations.