Castlethorpe Parish Council

# INFORMATION TECHNOLOGY (IT) POLICY

## 1. Purpose

This policy ensures all users understand how to use Council IT and data securely and legally. It protects the Council's systems and information, supports compliance with the Transparency Code**,** accessibility regulations, and current digital & data compliance expectations for smaller authorities

## 2. Scope

This policy applies to all councillors, employees, contractors, volunteers and third parties who access Council systems or data, whether on Council-owned or personal devices (BYOD). It covers hardware, software, cloud services, data handling, website publishing and communications.

## 3. Definitions

- Users – councillors, employees, contractors, volunteers, and third parties acting for the Council.
- Data – all digital information including (not limited to) documents, emails, images, recordings, personal data and accounting information.
- IT hardware/software – devices, operating systems, email and file services, collaboration tools, the Council website and any application or platform used for Council business.

## 4. Roles & Responsibilities

- The Council: owns this policy, adopts and reviews it annually, and ensures compliance is minuted for AGAR.
- Clerk (or delegated officer): day-to-day owner of IT controls; maintains asset and access records; coordinates incident response and ICO reporting when required.
- All Users: follow this policy and complete required training; promptly report incidents, losses, or suspicious activity.

## 5. IT Provision & Asset Management

- Council-provided devices, software, data access and services remain Council property and are recorded on the asset register.
- On leaving office/employment or ending work for the Council, Users must return all equipment within 14 days, in working order. Loss or damage may be recharged.
- Only authorised software may be installed. Licences must be valid and auditable.

## 6. Acceptable Use

- Use Council IT only for legitimate Council business.
- Do not attempt to bypass security controls, share accounts, or transfer Council data to unmanaged locations.
- Personal email or consumer cloud accounts must not be used for Council business.

**7. Access Control, Passwords & MFA**

To reduce account compromise risk and meet modern governance expectations:

• Passwords: minimum 12 characters, avoid reuse, and do not share.

• Multi-Factor Authentication (MFA): must be enabled on all Council email, file storage and admin accounts where available.

• Account lifecycle: joiners/leavers/amendments actioned promptly; access removed no later than the last working day.

• Administrator access: limited to named staff/councillors; use separate admin accounts.

**8. Device Security (Council-owned)**

• Must have automatic security updates enabled and supported operating systems only.

• Full-disk encryption and antivirus/anti-malware must be active.

• Local admin rights are restricted.

**9. BYOD (Use of Personal Devices)**

When personal devices are used for Council business, Users must:

• Enable device PIN/biometric lock and encryption; keep OS and apps up to date; run antivirus.

• Access Council email/files only through approved, managed apps or web portals (no local PST/unauthorised syncing).

• Permit remote removal of Council data from the personal device if access is withdrawn or the device is lost/stolen.

• Store Council data only in Council-approved locations (e.g., Microsoft 365/SharePoint/OneDrive tenant), not in personal cloud or messaging apps.

**10. Email & Communications**

• The Council will operate a Council-owned domain - @castlethorpe-pc.gov.uk

• All official communications must use Council mailboxes councillor and no forwarding to personal inboxes.

• Shared or role-based addresses (e.g., clerk@…) are required to ensure continuity when personnel change.

• Communications relating to Council business are public records. Users must keep them in Council systems so they can be found for FOI/EIR and retention**.**

**11. Data Protection & Data Handling**

• The Council processes personal data in line with UK GDPR and the Data Protection Act 2018;

• Data minimisation: collect and keep only what is necessary; store in approved locations; apply least-privilege access.

• Sharing: use secure methods; avoid sending personal data to personal emails or consumer platforms.

• Third-party processors: must have appropriate data processing agreements before any personal data is shared.

**12. Backup & Disaster Recovery**

- Council data stored in approved platforms is backed up using vendor or managed backup solutions with regular restore tests**.**
- Minimum expectations:
  - Daily automated backups of email/files;
  - Retention that meets the Retention Policy;
  - Quarterly restore tests with outcomes recorded to the Clerk.

**13. Website, Publishing & Accessibility**

- The Council website will publish required documents and keep them up to date per the Transparency Code for Smaller Authorities**.**
- The website must comply with the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 and meet WCAG 2.2 AA, with an up-to-date Accessibility Statement.
- A named person (Clerk or delegated webmaster) is responsible for content governance and regular accessibility checks.

**14. Cybersecurity & Phishing Protection**

- All devices used for Council business must have up-to-date antivirus and security updates.
- Users must complete basic cybersecurity awareness (including phishing and safe handling of personal data) on induction and at least annually thereafter.
- Suspicious emails or IT issues must be reported immediately to the Clerk.

**15. Incident Management & ICO Reporting**

- Report immediately to the Clerk any suspected: personal-data breach, compromised account, malware infection, lost/stolen device, or unauthorised disclosure.
- The Clerk will log the incident, contain the risk, assess impact, and decide whether to notify the ICO within 72 hours of becoming aware where feasible, and whether to notify affected individuals if there is high risk to their rights and freedoms. The Council will record all breaches, even if not reportable.
- The incident log will capture facts, decisions, mitigation, and lessons learned.

**16. Social Media & Online Behaviour (if used)**

- Only authorised Users may post to official Council social media.
- Use Council-controlled accounts; retain records in line with the Retention Policy; conduct remains professional and non-partisan.
- Do not discuss confidential matters or personal data in public channels.

**17. Procurement & Third Parties**

- New digital suppliers must meet Council security, accessibility and data-protection requirements, including WCAG 2.2 AA for public-facing services and appropriate data-processing terms.

**18. Risk Management, Insurance & Physical Security**

- The Council maintains insurance for IT equipment and records it on the asset register.
- Users must secure equipment from theft/unauthorised use; when travelling, do not leave devices in an unattended vehicle where avoidable; if unavoidable, store out of sight.
- Any loss or damage must be reported to the Clerk and Chair as soon as possible; criminal damage will be reported to the Police by the Clerk.
- Any loss of personal data resulting from device loss/theft must be escalated under Incident Management (Section 15).

**19. Training & Awareness**

- All Users will receive induction training on this policy, data protection**,** accessibility responsibilities for publishing, phishing awareness, and safe handling of personal data.
- Annual refresher training is available if required and completion is recorded.

**20. Monitoring & Compliance**

- The Council may review logs and configurations proportionately to investigate security incidents, fulfil legal obligations, and ensure policy compliance.
- Breaches of this policy may lead to disciplinary action (staff) or referral to the Monitoring Officer (members), and, if relevant, regulatory or criminal action.

**21. Policy Review & Governance**

- This policy is reviewed annually and re-adopted by resolution of the Council, with the review minuted

**22. Related Policies & References**

- Data Protection Policy; Document Retention Policy; Publication Scheme; Financial Regulations; Risk Register