HUNTINGTON PARISH COUNCIL

DATA PROTECTION AND INFORMATION SECURITY POLICY

Supporting policy to be read alongside the Council's General Privacy Notice

Status and purpose. This policy is intended to sit alongside the Council's existing General Privacy Notice. The Privacy Notice explains how the Council uses personal data and the rights of individuals; this policy sets out the practical controls and responsibilities for keeping Council information secure. It is a draft for the Council to review and adopt, not a replacement for the Privacy Notice.

Adopted: 21st October 2026
Review Date: 21st October 2031
Version: 1

1. Scope

This policy applies to all information created, received, stored or used for Huntington Parish Council ("the Council"), whether it is personal data, confidential Council information or other official records. It applies to councillors, the Clerk and other staff, volunteers, temporary workers, contractors and suppliers who are given access to Council information or systems.

It covers paper files, emails, meeting papers, finance and payroll records, resident correspondence, allotment or other service records, photographs, website content, cloud services, computers, phones, removable media and information discussed verbally. It should be read with the General Privacy Notice and relevant records-management, retention, subject access, breach-response and acceptable-use procedures.

2. Policy objectives

- Protect information against unauthorised access, disclosure, alteration, loss or destruction.
- Make sure information is accessed only by people who need it for an authorised Council purpose.
- Support the Council's obligations under the UK GDPR, Data Protection Act 2018 and other applicable requirements.
- Maintain the confidentiality, integrity and availability of Council records and essential services.
- Ensure security incidents are reported promptly, assessed, recorded and addressed.

3. Responsibilities

Full Council

- Approve this policy and provide oversight of information-security risks.
- Consider significant incidents and material risks and ensure appropriate action and resources.
- Ensure new systems or activities are assessed before they are introduced.

Parish Clerk / Proper Officer

- Coordinate implementation and maintain a record of key systems, authorised users, suppliers and security incidents.
- Arrange appropriate access, training, secure storage, backups and reviews.
- Coordinate incident response and data-protection assessments, escalating significant matters to the Chair and Council as appropriate.
- Ensure supplier arrangements and contracts address security and data protection where required.

All users

- Use Council information only for authorised Council work and follow this policy.
- Keep passwords and authentication methods confidential and do not share accounts.
- Protect Council information when working remotely, travelling or attending meetings.
- Report suspicious messages, lost devices, accidental disclosures and other possible incidents immediately.
- Return Council equipment and records, and stop accessing Council systems, when their role or authority ends.

4. Information classification and access

Information must be handled according to its sensitivity and the consequences of unauthorised disclosure. As a practical guide:

- Public: information formally approved for public release, such as published agendas, minutes and notices.
- Internal: routine working documents intended for Council use, not automatically for public release.
- Confidential/personal: personal data, staff matters, complaints, financial details, private contact information, draft decisions and confidential meeting papers.
- Restricted/high risk: account credentials, bank/payment details, sensitive personal data, safeguarding information, security configurations and information whose loss or disclosure could cause serious harm.

Access must be limited to what is necessary for a person's role. Confidential or restricted information must not be placed on public websites, open shared folders or unrestricted email distribution lists. Access permissions should be reviewed when responsibilities change and removed promptly when no longer needed. Classification does not override legal duties to publish, disclose or provide access to records.

5. Passwords, accounts and devices

- Use a separate account for Council work where possible and never share personal logins.
- Use long, unique passwords or passphrases. Use a reputable password manager and multi-factor authentication where available, particularly for email, cloud storage and administrator accounts.
- Lock screens when unattended and enable automatic screen locking.
- Keep operating systems, applications, browsers and security software updated; use supported devices and software.
- Do not disable antivirus, firewall, encryption or other security controls without authorisation.

- Do not install unapproved software or connect unknown USB/removable devices to Council equipment.
- Use device encryption and remote locking/wiping where supported, particularly for portable devices holding Council information.
- Report a suspected compromised account or lost device immediately and change credentials only through a trusted process.

6. Email and electronic communications

- Use the Council email account or other approved channel for Council business wherever provided. Personal email accounts are not permitted to be used to store or routinely conduct Council business.
- Before sending, check the recipient address, attachments and whether the recipient is entitled to receive the information.
- Must use **BCC or an approved mailing-list tool** when sending group emails where recipients should not see each other's addresses.
- Send sensitive information only using an approved secure method. If a message is sent to the wrong person, report it immediately; do not assume recall will remove all copies.
- Be alert to phishing, unexpected attachments, urgent payment requests, impersonation and changes to supplier bank details. Verify unusual requests using a known, separate contact route.
- Do not post personal or confidential information on social media or public forums. Council social-media activity must be authorised and follow the Council's communication arrangements.

7. Paper records, meetings and physical security

- Keep confidential papers in locked cabinets or secure rooms when not in use.
- Do not leave files, meeting papers or notes unattended in public places, vehicles or shared spaces.
- Collect printing promptly and use secure printing where available.
- Transport paper records discreetly and keep them under control. Report lost or misdirected documents immediately.
- Dispose of confidential paper using secure shredding or an approved confidential-waste provider.
- Keep keys, access codes and building credentials secure; report loss or suspected unauthorised entry.
- Take care with confidential discussions in public, at home or where family members or visitors may overhear.
- Before publishing agendas, minutes, reports or attachments, check whether personal data or confidential information should be redacted, while complying with transparency and access-to-information duties.

8. Remote working and personal devices

Council information may be accessed from a personal device only where this is authorised and appropriate safeguards are in place. Users must keep the device updated, locked and protected, avoid shared user profiles, prevent other household members from accessing Council records and ensure Council information is not automatically copied to personal cloud accounts or shared photo/file libraries. Information must not be stored on a personal device longer than necessary. The Clerk may require information to be removed from a device when access ends or a device is lost, subject to lawful records requirements.

Avoid public Wi-Fi for confidential work unless an approved secure connection is used. Do not use public or shared computers to access Council email or files.

9. Cloud services, backups and suppliers

Only services approved by the Council may be used to store or process Council information. Before a new system is adopted, the Council should consider access controls, multi-factor authentication, encryption, backups, service availability, data location, supplier support, breach notification, data export and deletion, and contractual terms.

- Keep backups of important records in a secure location separate from the primary system where practicable.
- Protect backups from unauthorised access, ransomware and accidental deletion, and periodically test that records can be restored.
- Maintain an up-to-date list of important systems and suppliers and who administers them.
- Before a supplier handles personal data, check the supplier's suitability and put the required written data-processing terms in place.
- Remove access and retrieve or securely delete information when a supplier's work ends, subject to retention and legal requirements.

10. Personal data breaches and security incidents

A security incident includes suspected or actual loss, theft, unauthorised access, disclosure, alteration or destruction of Council information. Examples include an email sent to the wrong person, a lost phone or paper file, a compromised account, malware, ransomware or unauthorised publication.

1. Report the incident immediately to the Parish Clerk. If the Clerk is unavailable or involved, report it to the Chair of the Council or the Council's designated alternative contact.
2. Give the known facts: what happened, when it was discovered, which information or systems may be involved, who may be affected and what actions have already been taken.
3. Take reasonable steps to contain the incident, such as securing an account or contacting the intended recipient, but do not destroy evidence or delay reporting while investigating.

4. The Clerk or authorised lead will record the incident, assess the risks, coordinate technical or supplier support and inform the Chair/Council as appropriate.
5. Where personal data is involved, assess whether the ICO must be notified without undue delay and, where feasible, within 72 hours of awareness if the breach is likely to risk individuals' rights and freedoms. Notify affected individuals without undue delay where the breach is likely to result in a high risk, unless a legal exception applies.
6. Record the decision and reasons even where notification is not required. Take remedial action and review lessons learned.

All incidents must be reported in good faith, including near misses. Users must not make public statements about an incident unless authorised.

11. Information sharing and publication

Before sharing information, confirm the recipient's identity and authority, the purpose and lawful basis, that the information is necessary and accurate, and that the transfer method is secure. Share only the minimum necessary. Use secure methods for sensitive or confidential material and document significant or recurring sharing arrangements where appropriate.

Information intended for publication should be checked before release. The Council must balance privacy and confidentiality with its statutory transparency and information-access duties. Where uncertain, seek advice from the Clerk and, where necessary, appropriate professional guidance before disclosing.

12. Retention, disposal and records management

Council records must be retained in line with the Council's Document Retention Policy and any applicable legal, financial, audit, archival or claims requirements. Users must not keep personal data indefinitely without a documented reason or delete records outside approved arrangements. When records reach the end of their retention period, they must be securely destroyed or anonymised. A legal hold, audit, investigation or information request may require routine destruction to be paused.

13. New systems, projects and risk assessment

Before introducing new software, cloud services, CCTV, monitoring, online forms or a new use of personal data, the Council should assess security, privacy, access, retention, supplier and continuity risks. A Data Protection Impact Assessment (DPIA) must be completed where the proposed processing is likely to result in a high risk to individuals. The Council should not proceed until significant risks and necessary safeguards have been considered and documented.

14. Training and compliance

Councillors, staff and relevant volunteers will receive guidance appropriate to their role, including secure email, phishing awareness, handling personal data, confidentiality and incident reporting. The Clerk will periodically review access, systems, suppliers and this policy, and provide compliance updates to the Council. Any suspected failure to comply will be considered promptly and may result in access being withdrawn or other appropriate action.

15. Reviewing the policy

The Council will review this policy at least annually and following a significant security incident, major system changes or relevant change in law or guidance. The review should confirm that the policy remains consistent with the General Privacy Notice and other Council procedures.