DATA PROTECTION & INFORMATION SECURITY POLICY

1. Purpose of the Data Protection & Information Security Policy

Henlow Parish Council recognises the importance of complying with its responsibilities under data protection legislation. This policy sets out how the Council protects and manages information including personal data in line with the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and sector best practice (from JPAG (Joint Panel on Accountability and Governance), NALC (National Association of Local Councils), SLCC (Society of Local Council Clerks).

This policy applies to all councillors, staff, contractors, and volunteers handling Council information and personal data, whether held electronically or in hard copy.

2. Legal and Regulatory Framework

The Council is committed to complying with the following:

- UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- AGAR requirements (including Assertion 10: Digital and Data Compliance)
- Relevant guidance from the Information Commissioner's Office (ICO), JPAG, NALC, and SLCC

3. Roles and Responsibilities

3.1 The Clerk is responsible for day-to-day information security and data protection.

3.2 All councillors, staff, contractors and volunteers ("Users") must follow this policy and report any security incidents or data breaches to the Clerk immediately.

3.3 Data Protection Officer (DPO): parish and town councils are exempt from the legal requirement to appoint a DPO under Section 7 of the Data Protection Act 2018. However, the Council may appoint a DPO if it chooses to do so. If appointed, the DPO will advise on data

protection obligations, monitor compliance, and act as the contact point for the ICO. The DPO can be another staff member other than the Clerk/RFO or an external provider.

4. Data Protection Principles

The Council will ensure that personal data held by the Council is:

- processed lawfully, fairly, and transparently: this means that personal information should only be collected from individuals if Users have been open and honest about why they want the information.
- collected for specified, explicit, and legitimate purposes.
- adequate, relevant, and limited to what is necessary: data will be regularly monitored so that only data that is needed will be held.
- accurate and kept up to date.
- kept only as long as necessary: data no longer needed will be removed electronically or physically shredded or securely disposed.
- processed securely: data will only be accessible by Users as absolutely necessary and cannot be accessed by members of the public.
- processed in accordance with the rights of individuals: individuals must be informed, upon request, of all the personal information held about them.

5. Information Security

The Council will ensure the following principles are adhered to:

- **Confidentiality**: Information is accessible only to authorised Users.
- **Integrity**: Information is accurate and complete.
- **Availability**: Information is accessible to authorised Users when required.

6. Information & Data Inventory

The Council will create and maintain an up to-date inventory of the information and personal data it holds across following locations including a classification by sensitivity and the protections in place for its security: -

- Computers, laptops, and mobile devices
- Software and cloud services
- Paper records
- Backups and portable media.

7. Access and User Management

7.1 Access to data and information is restricted to those who need it for Council business.

7.2 All devices and systems are password-protected with strong, unique passwords.

7.3 Access is removed promptly when a User leaves or changes role.

7.4 Use of a Council email account is mandatory for Council business**.**

8. Data Handling, Retention and Sharing

8.1 Personal data is to collected, used, and retained only as necessary for Council purposes, in line with the Council's Privacy Notice and Document Retention Policy.

8.2 Data is not to be shared with third parties except as required by law or with consent.

8.3 Backups will be made regularly, stored securely (including offsite/cloud), and tested periodically.

8.4 Data is to be securely deleted or destroyed when no longer required.

9. Digital and Data Compliance (AGAR Assertion 10)

The Council will take steps to ensure that it: -

- complies with all relevant digital and data protection laws, including the UK GDPR and Data Protection Act 2018.
- maintains an up-to-date inventory of all digital assets and ensures appropriate security controls are in place.
- restricts access to digital systems to authorised Users and requires the use of council email accounts for all council business.
- encrypts sensitive data and ensure regular, secure backups.
- conducts regular risk assessments and provides ongoing training to all Users.
- maintains clear procedures for reporting and responding to data breaches or cyber incidents.
- reviews its digital and data compliance processes annually and as part of the AGAR process.

10. Technical and Physical Security

The Council will take steps to ensure that: -

- all computers/laptops are protected by up-to-date anti-virus and firewall software.
- regular software and security updates are applied.
- data is encrypted where possible, especially on portable devices and backups.
- paper records are stored in locked cabinets or rooms.
- devices and media are securely wiped or destroyed before disposal.
- The Information Technology Policy is implemented and maintained, including Multi-Factor Authentication.

11. Incident Management and Breach Reporting

11.1 All security incidents, including data breaches, must be reported immediately to the Clerk (or DPO, if appointed).

11.2 Serious incidents must be reported to the Council and, where required, to the Information Commissioner's Office (ICO) within 72 hours.

11.3 The Council must maintain a log of any security incidents and carry out a review after such an incident to determine whether improvements can be made.

12. Training and Awareness

All Users must receive training on information security and data protection.

13. Review and Audit

13.1 The Council will conduct regular data audits and risk assessments.

13.2 Compliance with this policy will be monitored, and improvements are to be made as needed.

13.3 This policy will be reviewed every year, or more frequently if required by changes in legislation or following a security incident.

14. Relevant Policies

This policy should be read in conjunction with the Council's Privacy Notice and Document Retention Policy.

Revision History

Adopted at Full Council	**23 March 2026**
Due for review and readoption	**March 2027**