



Highley Parish Council –

Data Protection Policy (2026 Update)

To be adopted at the Annual Parish Council Meeting – 12 May 2026

1. Purpose

Highley Parish Council is committed to protecting the personal data it holds and ensuring compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

From the uploaded document:

“This policy sets out the council's commitment to data protection, and your rights and obligations in relation to personal data...”

This policy applies to **HR-related personal data** for job applicants, employees, workers, contractors and former employees. A separate Privacy Notice covers personal data processed for wider council business.

The **Clerk/RFO** is the Council's Data Protection Lead and is responsible for overseeing compliance.

2. Definitions

- **Personal Data:** Information relating to an identifiable living individual.
- **Processing:** Any operation performed on personal data, including collection, storage, use, disclosure or destruction.
- **Special Category Data:** Sensitive information such as health, ethnicity, political opinions, religious beliefs, sexual orientation, biometric data, and criminal records data.
- **Criminal Records Data:** Information relating to criminal convictions, allegations or proceedings.

3. Data Protection Principles

The Council processes HR-related personal data in accordance with the following principles.

Personal data must be:

1. **Processed lawfully, fairly and transparently**
2. **Collected for specified, explicit and legitimate purposes**
3. **Adequate, relevant and limited** to what is necessary
4. **Accurate and kept up to date**
5. **Retained only as long as necessary**
6. **Processed securely**, protecting against loss, misuse, unauthorised access or damage

From the uploaded document:

“The council will tell you of the personal data it processes... and the legal basis for processing in our privacy notices.”

4. Lawful Bases for Processing

The Council may process personal data where one or more of the following apply:

- Performance of a contract (e.g., employment contract)
- Compliance with a legal obligation
- Legitimate interests of the Council or a third party
- Protection of vital interests
- Performance of a task carried out in the public interest or under official authority

Where none of these apply, **consent** will be sought. Consent may be withdrawn at any time.

The Council will not use personal data for unrelated purposes without notifying the individual and identifying the lawful basis.

5. Processing Special Category Data

Special category data will only be processed where permitted by law, including:

- Employment law obligations
- Vital interests
- Data made public by the individual
- Legal claims
- Occupational health purposes

- Substantial public interest
- Public health
- Archiving or research purposes

Where required, explicit consent will be obtained.

6. Data Storage, Accuracy and Sharing

- HR-related personal data is stored securely in both electronic and hard-copy formats.
- Individuals must notify the Council of any changes to their personal information.
- Personal data may be shared with contractors or agents where necessary for contractual or legitimate purposes.
- Third parties must comply with data protection law and process data only under the Council's instructions.

From the uploaded document:

“Sometimes the council will share your personal data with contractors and agents... We require those individuals or companies to keep your personal data confidential and secure.”

7. Individual Rights

Individuals have the following rights:

- Access to their personal data
- Rectification of inaccurate data
- Erasure of data in certain circumstances
- Restriction of processing
- Objection to processing based on legitimate interests
- Data portability (where applicable)
- The right to complain to the **Information Commissioner's Office (ICO)**

Subject Access Requests (SARs)

- Requests must be submitted to the **Clerk or Chair**.
- Proof of identity may be required.
- The Council will respond within **one month**, unless the request is complex.
- Excessive or repeated requests may incur a reasonable administrative fee.

8. Data Security

The Council takes data security seriously and maintains appropriate technical and organisational measures to protect personal data.

This includes:

- Access controls and password protection
- Secure storage and destruction of documents
- Staff awareness and confidentiality obligations
- Restrictions on removing personal data from Council premises
- Prohibition on storing personal data on personal devices

From the uploaded document:

“Individuals who have access to personal data are required to access only data that you have authority to access and only for authorised purposes...”

9. Data Protection Impact Assessments (DPIAs)

Where processing is likely to result in a high risk to individuals’ rights and freedoms (e.g., CCTV monitoring), the Council will undertake a DPIA to assess necessity, proportionality and risk mitigation.

10. Data Breaches

The Council maintains procedures to detect, report and investigate data breaches.

- All breaches must be reported immediately to the Clerk or Chair.
- Evidence relating to the breach must be preserved.
- If a breach poses a risk to individuals’ rights and freedoms, the Council will notify the **ICO within 72 hours**.
- Where a breach presents a high risk, affected individuals will be informed.

From the uploaded document:

“The council will record all data breaches regardless of their effect.”

11. International Data Transfers

The Council will not transfer HR-related personal data outside the UK or EEA unless lawful safeguards are in place.

12. Responsibilities of Individuals

All staff, councillors and contractors must:

- Keep personal data accurate and up to date
- Access only data they are authorised to access
- Keep data secure
- Not disclose data without proper authority
- Not store data on personal devices
- Report concerns or breaches immediately

Failure to comply may result in disciplinary action.

13. Training

The Council will provide training to ensure all individuals understand their responsibilities under this policy. Those handling personal data regularly will receive additional training.

14. Review and Adoption

This policy will be:

- Adopted at the **Annual Parish Council Meeting on 12 May 2026**
- Reviewed annually
- Updated sooner if required by changes in legislation or best practice