# Shadingfield, Sotterley, Willingham, and Ellough Joint Parish Council

# Data Protection Policy Updated 2026

## Policy Statement

The council remains committed to transparency in how it collects, uses, stores and disposes of personal data relating to staff and workers. This policy sets out the council's obligations under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018 (DPA 2018)** and explains the rights of individuals whose data we process.

This policy applies to personal data relating to **current and former job applicants, employees, workers, contractors and former employees** ("HR-related personal data"). It does **not** apply to personal data processed for wider council business or members of the public.

The council has appointed Vicki Ellis, Clerk and RFO, as the Data Protection Lead responsible for compliance.

## Definitions

- **Personal data**: Any information relating to an identifiable living individual.
- **Processing**: Any operation performed on personal data, including collection, storage, use, disclosure or destruction.
- **Special category data**: Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation, and genetic or biometric data.
- **Criminal offence data**: Information relating to criminal convictions, allegations or proceedings.

## Data Protection Principles

The council processes HR-related personal data in accordance with the **seven principles of UK GDPR**:

1. **Lawfulness, fairness and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality (security)**

7. **Accountability**

The council maintains a **Record of Processing Activities (ROPA)** as required under UK GDPR.

## Legal Bases for Processing

### Personal Data

The council processes personal data only where one or more lawful bases apply:

- performance of a contract
- compliance with a legal obligation
- legitimate interests
- vital interests
- performance of a public task / exercise of official authority

Consent is only used where no other lawful basis applies.

## Special Category Data

Processing occurs only where a lawful basis **and** a special category condition apply, including:

- employment law obligations
- vital interests
- data made public by the individual
- legal claims
- occupational health
- substantial public interest
- public health
- archiving or research

## Processing and Data Sharing

- HR data is stored securely in personnel files, HR systems and secure servers.
- Retention periods are set out in the council's **Data Retention Policy**.
- Data may be shared with contractors or processors only where necessary and subject to written agreements compliant with UK GDPR.

## Individual Rights

Under UK GDPR, individuals have the right to:

- access their data (Subject Access Request)
- rectification
- erasure ("right to be forgotten")
- restriction of processing
- objection
- data portability (added for UK GDPR compliance)
- not to be subject to solely automated decision-making

## Subject Access Requests (SARs)

- Requests must be responded to within **one month**.
- Extensions of up to two months may be applied for complex requests.
- Identity verification may be required.
- Repeated or excessive requests may incur a reasonable fee.

## Data Security

The council implements appropriate **technical and organisational measures**, including:

- secure storage and controlled access
- password protection and multi-factor authentication where available
- encrypted devices
- secure disposal of confidential waste
- staff training and access controls

Employees must:

- access only authorised data
- keep data secure
- not remove personal data without authorisation
- not store council data on personal devices unless authorised and protected
- report any concerns immediately

## Data Protection Impact Assessments (DPIAs)

A DPIA is required where processing is likely to result in **high risk**, including:

- CCTV monitoring
- new technologies
- large-scale processing of sensitive data

## Data Breaches

- All breaches must be recorded.
- Breaches posing a risk to individuals must be reported to the ICO within **72 hours**.
- High-risk breaches must be reported to affected individuals without undue delay.
- Staff must report breaches immediately to the Clerk.

## International Transfers

Updated for post-Brexit law:

The council will not transfer HR-related personal data outside the **UK** unless:

- an adequacy regulation is in place, or
- appropriate safeguards (e.g., ICO-approved IDTA or UK Addendum) are used.

## Individual Responsibilities

Employees must:

- keep their personal information up to date
- follow all council data protection policies
- report concerns or breaches immediately
- never transfer data internationally without authorisation

Failure to comply may result in disciplinary action.

## Adoption and Review

**Date of adoption:** May 2026
**Date of next review:** 2028
**Chair:** R. Ellis
**Clerk:** V. Ellis