Cornsay Parish Council

DATA PROTECTION POLICY

ADOPTED FEBRUARY 2026

To operate efficiently, the Council must collect and use information about the people and organisations it works with. This may include members of the public, current, former and prospective employees, customers, contractors, suppliers, and partner organisations.

The lawful and appropriate handling of personal information is critical to the Council's operations and to maintaining trust and confidence with those it does business with. The Council is committed to ensuring that all personal information is processed fairly, lawfully, and in accordance with applicable data protection legislation.

The Council is registered with the Information Commissioner's Office as a Data Controller.

Overall responsibility for compliance with this policy rests with the Council. Day-to-day responsibility is delegated to the Clerk, who is responsible for carrying out information audits, managing the personal information held by the Council, issuing privacy notices, handling data protection requests and complaints, and ensuring the secure retention and disposal of information.

Councillors who process personal data in an individual capacity, and not on behalf of the Council, may be considered Data Controllers in their own right and may therefore be required to register with the Information Commissioner's Office.

All councillors and officers who hold or process personal data are responsible for complying with data protection legislation and must ensure that personal and sensitive information is handled in accordance with this policy.

Legal Duties

Data Protection Framework

The UK General Data Protection Regulation (UK GDPR) sits alongside the Data Protection Act 2018 and governs the processing of personal data. The legislation applies to personal data, meaning any information relating to an identified or identifiable living individual.

Processing refers to any operation performed on personal data, including collection, recording, storage, use, sharing, or deletion. The Parish Council holds personal data relating to living individuals and processes such data as necessary to carry out its functions and responsibilities.

Data Protection Principles

When handling personal data, all staff, councillors, and volunteers must ensure that the following principles are complied with:

- **Processed fairly and lawfully**
  Staff, councillors, and volunteers will be open and transparent about why personal information is required and how it will be used.
- **Processed for specified purposes only**
  Personal data will be collected only for clear, legitimate purposes and will not be used in ways incompatible with those purposes.
- **Adequate, relevant, and limited to what is necessary**
  Only the personal data needed for the intended purpose will be collected and retained. Data will be reviewed to ensure that neither excessive nor insufficient information is held.
- **Accurate and kept up to date**
  Reasonable steps will be taken to ensure personal data is accurate. Any data found to be inaccurate will be corrected or deleted without delay.
- **Not kept longer than necessary**
  Personal data will be retained only for as long as required for the purpose for which it was collected, in line with the Council's retention schedule.
- **Processed in accordance with individuals' rights**
  Individuals have the right to request access to their personal data and will be provided with information held about them in accordance with data protection legislation.
- **Kept secure**
  Appropriate technical and organisational measures will be in place to protect personal data from unauthorised access, loss, or disclosure.

Lawful Bases for Processing Personal Data

The lawful bases for processing personal data are set out in Article 6 of the UK GDPR. At least one lawful basis must apply before personal data is processed:

- **(a) Consent**
  The individual has given clear and informed consent for their personal data to be processed for a specific purpose.
- **(b) Contract**
  Processing is necessary for the performance of a contract with the individual, or to take steps at the individual's request prior to entering into a contract.
- **(c) Legal obligation**
  Processing is necessary to comply with a legal obligation to which the Council is subject (excluding contractual obligations).
- **(d) Vital interests**
  Processing is necessary to protect someone's life.
- **(e) Public task**
  Processing is necessary to perform a task carried out in the public interest or in the exercise of official authority, with a clear basis in law.
- **(f) Legitimate interests**
  Processing is necessary for the legitimate interests of the Council or a third party, except where those interests are overridden by the individual's rights and freedoms.

Information Held by the Council

The Council retains certain information in order to carry out its day-to-day operations, achieve its objectives, and comply with its legal and regulatory obligations. In most cases, the personal data

held is limited to basic contact information, such as names, addresses, telephone numbers, and email addresses. More detailed personal data is held only where necessary, for example in relation to employees.

In the normal course of its business, the Council may receive and process personal data in connection with the following activities:

- administration of Parish Council meetings
- administration and management of Council facilities
- administration of employment and staffing matters
- management of councillor membership and related records
- receiving, recording, and responding to correspondence
- management of contractual arrangements
- receiving and processing grant applications
- creating and maintaining volunteer lists for specific activities
- responding to contact made via the Parish Council website or social media channels
- processing PAYE reporting and related submissions to HMRC

Storage and Retention of Data

Paper records held by the Council are stored securely, and electronic records are held on password-protected computer systems with appropriate anti-virus and security software. Access to personal data is restricted to authorised persons only and is not available to members of the public.

Personal data is retained only for as long as it is required for the purpose for which it was collected and in accordance with the Council's retention policy. Once data is no longer required, is out of date, or has fulfilled its purpose, and the applicable minimum retention period has expired, it will be securely deleted or destroyed.

Use and Sharing of Personal Data

Personal data will be used only for the purpose for which it was collected. The Council will not disclose personal data to third parties without the explicit consent of the data subject, unless disclosure is required or permitted by law. The Council does not sell personal data.

Where a councillor requires access to personal data in order to carry out their official duties, access will be limited to the minimum information necessary for the specific task and the data must be used solely for that purpose. Personal data will not be shared or released without the prior knowledge or authorisation of the Clerk.

Personal data will not be used for political purposes unless the data subject has given explicit consent.

Rights of Individuals

Anyone whose personal data is processed by the Parish Council has the right to:

- be informed about what personal data is held about them
- understand why their personal data is being processed
- know, where applicable, who their personal data has been shared with
- know how to access their personal data
- have their personal data kept accurate and up to date
- understand how the Council complies with data protection legislation
- access their personal data in accordance with data protection law

- restrict or object to the processing of their personal data in certain circumstances
- request the correction, rectification, or erasure of inaccurate or unlawful personal data

Anyone wishing to obtain further information about the personal data held by the Council, or to request access to, correction of, or erasure of their personal data, should contact the Clerk.

The Council will respond to all valid requests as promptly as possible and, in any event, within the statutory timescales set out in data protection legislation.

Requests for Erasure of Personal Data

Individuals have the right to request the erasure of their personal data where it is no longer necessary for the purpose for which it was originally collected, or where another lawful ground for erasure applies under data protection legislation.

Where a request for erasure is received, the Clerk will respond to the request and has delegated authority from the Council to arrange for the secure deletion of personal data where appropriate.

If a request is considered to be manifestly unfounded or excessive, the Council may refuse to act on the request or may charge a reasonable fee, in accordance with data protection legislation. Any such fee will be determined in line with the Council's Publication Scheme. The Parish Council will be informed where a request is refused or a fee is charged.

Data Protection Officer

The GDPR does not define a parish council as a public authority therefore does not require it to appoint a Data Protection Officer.

Data Breaches

Any actual or suspected personal data breach identified by the Council, or reported to it, must be reported immediately to the Clerk. The Clerk has responsibility for investigating personal data breaches and will conduct an investigation with the support of the Parish Council where appropriate.

Investigations will be commenced promptly and completed without undue delay, with initial assessment taking place as soon as possible following notification of the breach.

Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Clerk will notify the Information Commissioner's Office (ICO) without undue delay and, where required, within 72 hours of becoming aware of the breach. Such risks may include, for example, discrimination, damage to reputation, financial loss, loss of confidentiality, or other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Clerk will also ensure that affected individuals are informed without undue delay.

The Clerk will maintain procedures to detect, report, investigate, and record personal data breaches.

As part of managing a breach, the Clerk may take further action as appropriate, including:

- isolating affected computer systems or IT equipment
- informing councillors as necessary
- notifying affected individuals
- seeking external technical or legal assistance to assess the breach
- reporting the breach and its outcome to the Council and recommending any necessary remedial actions or policy reviews

Data Map

The Council holds data for a variety of reasons and processes it in accordance with the relevant lawful basis.

Purpose	Categories of data	Sharing	Data Processors	Third countries that data is shared to	Retention	Lawful basis for processing	Condition for processing special category data
Minutes	Identity Contact info	N/A	Cloud storage provider Website provider	EU USA	Indefinite	Legal obligation	
Accounts	Identity Contact info Bank details	HMRC	Cloud storage provider Website provider	EU USA	6 years	Legal obligation	
Correspondence and casework	Identity Contact info Special category data	Other local authorities Law enforcements	Cloud storage provider Website provider	EU USA	3 years	Public task	Substantial Public Interest
Payroll	Identity Contact info Bank details	HMRC	Cloud storage provider	EU USA	6 years	Legal obligation	
HR info	Identity Contact info Special category data	N/A	Cloud storage provider	EU USA	3 years after employment ends	Contract	Employment, social security and social protection
Acceptance of Office forms	Identity	N/A	N/A	N/A	Indefinite	Legal obligation	
Register of Interests	Identity Contact info Special category data	Other local authorities (monitoring officer)	Cloud storage provider	EU USA	Term of office	Legal obligation	Substantial Public Interest
Planning applications	Identity Contact info	Other local authorities	Cloud storage provider	EU USA	3 years	Public task	
Grant applications	Identity Contact info	N/A	Cloud storage provider	EU USA	3 years	Consent	
Newsletters	Identity Contact info	N/A	Mailing list provider	EU	As long as necessary	Consent	

Appropriate Policy Document

Where the Council processes special category personal data, it maintains an Appropriate Policy Document. This document explains how such data is processed and the measures in place to ensure compliance with data protection legislation.

Special Category Personal Data

Special category personal data includes information relating to a person's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data (for the purpose of uniquely identifying a natural person)
- health
- sex life or sexual orientation

Conditions for Processing Special Category Data

The Council processes special category personal data only where a lawful condition under Article 9 of the UK GDPR applies.

Article 9(2)(a) – Explicit consent

Where explicit consent is required for specific purposes, the Council ensures that such consent is:

- freely given, specific, informed, and unambiguous
- provided by a clear affirmative action
- recorded and retained as evidence of the lawful condition for processing

Examples of this processing include health information provided by individuals who require reasonable adjustments to access Council services, or data supplied by individuals participating in surveys or subscribing to Council updates or newsletters.

Article 9(2)(b) – Employment, social security, and social protection (where authorised by law)

The Council may process special category data where it is necessary to comply with obligations or exercise rights conferred by law in connection with employment, social security, or social protection.

Examples include processing data in connection with the provision of social services to residents or the Council's responsibilities as an employer.

Article 9(2)(e) – Data made public by the data subject

The Council may process special category personal data where the data has been manifestly made public by the individual concerned.

Article 9(2)(f) – Legal claims and judicial acts

Processing may take place where it is necessary for the establishment, exercise, or defence of legal claims.

Examples include litigation and employment tribunal proceedings.

Article 9(2)(g) – Substantial public interest (with a basis in law)

The Council may process special category data where it is necessary for reasons of substantial public interest and where there is a clear legal basis for doing so, including in the delivery of public services.

Examples include information obtained or used when investigating complaints, or when responding to requests made under the Freedom of Information Act 2000 or the Environmental Information Regulations.

Procedures for Ensuring Compliance with the Data Protection Principles

The Council has implemented the following procedures to ensure compliance with the data protection principles when processing special category personal data.

Principle (a) – Lawfulness, fairness, and transparency

Processing of special category and criminal offence data is carried out lawfully, fairly, and transparently. The Council:

- identifies and documents an appropriate lawful basis under Articles 6, 9, and 10, and a relevant Schedule 1 condition where required
- provides clear and accessible privacy information explaining why and how such data is processed

Processing carried out for substantial public interest purposes is necessary for the exercise of the Council's statutory functions. Processing for employment purposes relates directly to the Council's obligations as an employer.

Principle (b) – Purpose limitation

The Council clearly identifies its purposes for processing special category data and includes these in its privacy information. Where data is to be used for a new purpose, the Council will assess compatibility with the original purpose or seek specific consent where required.

Special category data may be processed for substantial public interest purposes where necessary to:

- fulfil statutory functions
- comply with, or assist others to comply with, regulatory requirements
- establish whether unlawful or improper conduct has occurred
- protect the public from dishonesty
- prevent or detect unlawful acts
- disclose information to elected representatives where lawful

Where appropriate and lawful, special category data collected for one of these purposes may be used for another listed purpose, provided the processing is necessary and proportionate.

When sharing data:

- with another controller, the Council will document that the recipient is authorised by law to process the data
- with a processor, the Council will ensure that processing arrangements and purposes are clearly documented in a contract and data processing schedule

Special category data will not be processed for purposes that are incompatible with those for which it was originally collected.

Principle (c) – Data minimisation

The Council collects and processes only the special category data that is necessary and proportionate for its stated purposes. Any special category data that is received or obtained but is not relevant to those purposes will be securely erased.

Principle (d) – Accuracy

Where the Council becomes aware that special category data is inaccurate or out of date, it will take all reasonable steps to ensure that the data is corrected or erased without undue delay, taking account of the purpose for which it is processed.

Principle (e) – Storage limitation

Special category data processed for employment or substantial public interest purposes is retained only for the periods set out in the Council's retention schedule, unless longer retention is required for lawful archiving purposes.

Retention periods are determined by reference to legal obligations and operational necessity. The retention schedule is reviewed regularly and updated as required.

Principle (f) – Integrity and confidentiality (security)

The Council assesses risks to special category data and implements appropriate technical and organisational measures to ensure its security. These measures are reviewed and updated regularly to maintain their effectiveness.