EAST SUTTON PARISH COUNCIL

DATA PROTECTION POLICY

Introduction

East Sutton Parish Council (the Council) is committed to compliance with the data protection law applicable to its collection, storage and use of information about individuals.

This can include parishioners, members of the public, suppliers, business contacts, employees and other people the Council has a relationship with or may need to contact.

This policy describes how such personal data must be collected, handled and stored to meet the Council's data protection standards and comply with the law.

Key definitions

Personal Data: any information relating to an identified or identifiable living individual, (a 'data subject'). This includes names, addresses, email addresses, telephone numbers and other information that can identify a person.

Special Category Data: personal data revealing among other categories, racial or ethnic origin, religious or philosophical beliefs and health data. This data requires additional protections.

Data Controller: the organisation that determines the purpose and the means of processing personal data. East Sutton Parish Council is the data controller for the personal data it processes.

Data Processor: an organisation that processes personal data on behalf of the data controller. This may include IT contractors, or other third-party service providers.

Data Protection Law

The UK General Data Protection Act (UK GDPR) and the Data Protection Act 2018, (as amended by the Data Use and Access Act 2025) provide the current legal framework in the United Kingdom, regulating how organisations including the Council, must collect, handle and store personal data.

These rules apply to all personal data processed by the Council, regardless of whether data is stored electronically, on paper or in other formats.

To comply with the data protection law, personal data must be collected and used fairly, stored safely and not disclosed unlawfully.

The UK GDPR is underpinned by seven important principles. These state that personal data must be:

1) processed fairly, lawfully and transparently
2) collected only for specific, lawful purposes
3) adequate, relevant and limited to what is necessary
4) accurate and where necessary, kept up to date
5) held for no longer than necessary
6) processed securely; and

7) that the Controller is accountable for demonstrating compliance with the principles

Lawful basis for processing

Under the UK GDPR, the Council must identify a lawful basis for all processing of personal data. The Council relies upon the following lawful bases:

• **Public Task** The Council processes personal data in the performance of its functions as a public authority. This includes processing data for:
◦ Council administration and governance
◦ Planning reviews and consultation responses
◦ Management of Council assets and services
◦ Responding to enquiries from parishioners and other residents
◦ Maintaining the register of councillors
◦ Preparing and publishing agendas and minutes

• **Legal Obligation**: Processing necessary to comply with legal obligations including:
◦ Employment law requirements
◦ Health and safety obligations
◦ Financial record keeping and audit requirements
◦ Freedom of Information Act requests
◦ Transparency requirements

• **Contract**: Processing necessary for contracts with:
◦ Employees
◦ Suppliers and contractors
◦ Service providers

C**onsent:** used only where no other lawful basis applies and provided it is freely given, specific, informed and unambiguous, such as when obtained for purposes such as:
◦ Emailing the parish newsletter
◦ Photographs for promotional purposes
◦ Optional surveys or consultations

• **Legitimate Interests** – may be used where the processing is necessary for the legitimate interests pursued by the Council, provided this does not override the rights and interests of the data subjects.

Where the Council processes Special Category Data, e.g. health or diversity information, an additional lawful processing condition must be met, such as:
◦ explicit consent; or
◦ employment, and social protection law; or
◦ substantial public interest under UK law, (for example. Health & Safety)

People, risks and responsibilities
This policy applies to:
• East Sutton Parish Council (Elected members)
• ultimate responsibility for ensuring the Council meets its data protection obligations

• approval of data protection policies and procedures
• ensuring adequate resources are allocated for data protection compliance.

• Parish Clerk (Proper Officer)
• day-to-day implementation of data protection policies and processes
• ensuring staff and councillors receive appropriate data protection training
• handling subject access and other rights requests
• reporting data protection issues to the Council
• ensuring privacy notices are kept up to date
• administering appropriate data processing agreements with third parties

• The officer in charge of IT is responsible for:
• ensuring all systems, services and equipment used for storing data meet acceptable security standards.
• performing regular checks and scans to ensure security hardware and software is functioning properly.
• evaluating any third-party services the Council is using or considering using to store or process data. For example, cloud computing services.
• reporting any security incidents to the Parish Clerk

• All staff and volunteers of East Sutton Parish Council
Everyone who works for East Sutton Parish Council has some responsibility for ensuring personal data is collected stored and handled appropriately in compliance with this policy.

• All contractors, suppliers and other organisations working with or on behalf of the Council
• ensuring data is only processed on documented instructions from the Council
• maintaining appropriate security measures
• assisting, where necessary, the Council in facilitating the response to data subject rights requests
• notifying the Council of any personal data breach without undue delay.

General officer guidelines
• The only people able to access data covered by this Policy should be those who need it for their role.
• Personal data should not be shared informally.
• The Council will provide training to all elected members and employees to help them understand their responsibilities when handling personal data.
• Officers should keep all personal data secure, by taking sensible precautions and following the guidelines below, in particular:
• strong passwords must be used, and they should never be shared.
• personal data should not be disclosed to unauthorised people, either within the Council or externally.
• Suspicious emails or security incidents or suspected personal data breaches must be reported to the Clerk immediately.
The Council must notify personal data breaches to the Information Commissioners Office (ICO) within 72 hours of becoming aware of the breach.
• Personal data must be regularly reviewed and updated if it is found to be out of date or if no longer required it should be deleted and securely disposed of.

- Officers should request help if they are unsure about any aspect of data protection.

Data use

Personal data processed by the Council should be limited to what is necessary for the purpose, accessible only to those officers who need access in order to perform their duties and held only for as long as is necessary for that purpose. All processing must respect the integrity and confidentiality of the data. For example:

- When working with personal data, officers should ensure the screens of their computers are always locked when left unattended.

- Personal data should not be shared informally. In particular it should not be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically.

- Personal data should never be transferred outside of the UK and European Economic Area in the absence of a prior assessment of the risk and, where necessary the implementation of required legal adequacy mechanisms.

- Officers should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the officers responsible for data protection and IT.

Data stored on paper

Manual records including printouts should be kept in a secure place, such as a locked drawer or cabinet and all printouts should be promptly retrieved from printers. Paper records should be securely disposed of when no longer required, such as by shredding or disposal in provided confidential waste bins.

Data stored electronically

Electronic records must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords that are changed regularly and never shared between officers.

- Data should only be stored on designated drives or servers and should only be uploaded to approved cloud/server computing services.

- Servers containing personal data should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those backups should be tested regularly, in line with standard backup procedures.

- Data should never be saved directly to laptops or other mobile devices like memory sticks, tablets or smartphones.

- All servers and computers containing data should be protected by approved security software and a firewall.

Data accuracy

The Council must take reasonable steps to ensure that data is kept accurate and up to date. The more important it is that personal data is accurate, the greater the effort the Council should put into ensuring its accuracy.

It is the responsibility of all officers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Officers should not create any unnecessary additional data sets.

- Officers should take every opportunity to ensure data is updated. For instance, by confirming parishioner or supplier details when they call.

- The Council will seek where appropriate, to make it easy for data subjects to update the information the Council holds about them. for instance, via the Council website.

- Data should be updated as inaccuracies are discovered. For example, if a contact can no longer be reached on their stored details, then they should be removed from the database.

Individual Rights

Under UK GDPR, data subjects have the following rights. The Council will facilitate these rights and respond to requests within the required time frames.

- **Right to be informed** – individuals have the right to be informed about the collection and use of their personal data. The Council will provide privacy notices at the point of data collection.
- **Right of Access** (Subject Access Request) – data subjects have a right to obtain confirmation that their data is being processed and to access their data. Requests are free of charge (except where manifestly unfounded or excessive) and must be responded to within one month (extendable by up to two further months for complex requests)
- **Right to rectification** – data subjects have the right to have inaccurate personal data corrected.
- **Right to erasure** – data subjects may request deletion of their data in certain circumstances.
- **Right to restrict Processing** – data subjects may request restriction of processing where for example they contest the accuracy of the data (pending verification).
- **Right to data Portability** – data subjects can, in certain cases, request their data is provided in a structured, machine-readable format and to have that data transmitted to another provider.

• **Right to object** – data subjects have the right in certain circumstances to object to the processing of their data, for example for direct marketing or where based on legitimate interest grounds (unless compelling grounds to continue processing exist).
The Council will respond to requests without undue delay and within the legally required time frame (usually one month) and provide information free of charge (except in exceptional circumstances). The Council will explain any refusal and inform the data subject of their right to complain to the Council and, ultimately to the regulator, the ICO.
The Proper Officer will always take appropriate steps to verify the identity of anyone making a rights request before responding.

Disclosing data for any other reasons
Before disclosing any personal data, the Council will verify the identity of the requestor and consider the lawful basis for their request and for any disclosure.
This will include considering whether data subject consent is required or whether other lawful grounds exist (such as where required by law, the order of a court or where disclosure is to law enforcement agencies and necessary for crime prevention or detection purposes).
In all such cases, the Proper officer will ensure the request is legitimate, in conjunction with the Chairman of the Council and the Council's legal advisers where necessary.

Adopted on: 07/01/2026