



HORSMONDEN PARISH COUNCIL

Data Protection Policy

Horsmonden Parish Council: Data Protection Policy

Document control

Item	Detail
Organisation	Horsmonden Parish Council, Parish Office, Horsmonden Village Hall, Back Lane, Horsmonden, Kent, TN12 8LH
Policy owner	The Council (accountable), administered by the Clerk
Version	2.0 (full redraft replacing the version approved 1 September 2025)
Approved by	Full Council, minute ref [to be added] on [date]
Next review	Annually, or sooner if the law or the Council's processing changes
Related documents	Privacy Notices; Document Retention Policy; Data Breach Procedure; Subject Access Request Procedure; Data Protection Complaints Procedure; CCTV Policy and DPIA; Data Map and Assessment of personal Data Held, IT and Email Policy

1. Introduction

Horsmonden Parish Council ("the Council") is a data controller. It holds personal data about residents, councillors, employees, volunteers, suppliers, hirers, allotment holders, correspondents and other members of the public so that it can carry out its statutory functions and run its services.

This policy sets out how the Council complies with data protection law and what councillors, staff and volunteers must do when they handle personal data on the Council's behalf. It is written for internal use. Information for the public about how their data is used is published separately in the Council's Privacy Notices.

The Council must consult its Data Protection Officer (DPO) before starting any significant new processing activity, or changing an existing one, so that compliance steps (including any Data Protection Impact Assessment) are addressed at the outset.

2. Scope and legal framework

This policy applies to all councillors, employees, volunteers and anyone else who processes personal data on the Council's behalf, in any format (paper, electronic, audio, CCTV) and on any device, including personal devices used for Council business.

The Council processes personal data in accordance with:

- the UK-GDPR
- the Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025
- the Privacy and Electronic Communications Regulations 2003 (PECR), for electronic communications
- guidance and codes of practice issued by the Information Commissioner's Office (ICO), the UK supervisory authority.

Related rights of access to Council information (the Freedom of Information Act 2000 and the Environmental Information Regulations 2004) are dealt with under the Council's separate policies.

3. Definitions

Personal data: any information relating to an identified or identifiable living individual (a "data subject"). Examples held by the Council include names, addresses, email addresses, telephone numbers, correspondence, bank details, payroll and HR records, allotment and burial records, booking records, CCTV images and online identifiers.

Special category data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data used to identify someone, data concerning health, and data concerning a person's sex life or sexual orientation. It needs extra protection and an additional legal condition (section 5.3).

Criminal offence data: personal data relating to criminal convictions and offences or related security measures, including allegations and proceedings. It is treated separately from special category data (section 5.4).

Processing: anything done with personal data, including collecting, recording, storing, using, sharing, viewing, archiving and destroying it.

Controller: the organisation that decides why and how personal data is processed. For Council business, the controller is Horsmonden Parish Council as a corporate body, not individual councillors or officers.

Processor: an organisation that processes personal data on the Council's behalf and under its instructions (for example, a payroll bureau, IT support provider or cloud service).

Personal data breach: a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. Roles and responsibilities

The Council as controller is accountable for compliance and must be able to demonstrate it. Day-to-day responsibilities are allocated as follows.

4.1 The Council

- Adopts and reviews this policy and related procedures.
- Ensures adequate resources, training and security are in place.
- Takes decisions on new or changed processing after considering the DPO's advice.

4.2 The Clerk (Proper Officer)

The Clerk, Mrs. L. Noakes, is responsible for implementing this policy day to day, supported by the Deputy Clerk, Mrs. A. Blyth. This includes:

- maintaining the Record of Processing Activities, Retention Schedule and Privacy Notices
- logging, coordinating and responding to requests from individuals to exercise their rights, and to data protection complaints, within the legal time limits
- ensuring Council systems, devices and services meet appropriate security standards, and that backups and access controls are in place
- assessing third-party and cloud services before use, and putting compliant contracts in place with processors
- recording and managing personal data breaches, and deciding on ICO notification
- consulting the DPO in each of the above where advice is needed.

4.3 Councillors

Councillors who handle personal data for Council business do so on behalf of the Council and must follow this policy. In particular, councillors must:

- use their Council email account (horsmonden-pc.gov.uk) for all Council business, not personal accounts
- keep Council information on personal devices secure, and delete it when no longer needed or when they leave office
- not disclose personal data received in confidence, including information from closed (Part 2) sessions
- pass any request, complaint or suspected breach to the Clerk immediately.

A councillor acting in a political or ward capacity (for example, as a party candidate) may be a separate controller for that activity and is personally responsible for it.

4.4 Employees and volunteers

All employees and volunteers must handle personal data in line with this policy, access only the data they need for their role, and report any request, complaint or suspected breach to the Clerk without delay.

4.5 Data Protection Officer

The Council's DPO is Richard Newell of GDPR-Info Ltd, appointed under Article 37 UK-GDPR. The DPO can be contacted directly via the Clerk (clerk@horsmonden-pc.gov.uk, 01892 724989). The DPO's tasks (Article 39) are to:

- inform and advise the Council, councillors and staff of their data protection obligations
- monitor compliance with data protection law and this policy, including audits, training and awareness
- advise on Data Protection Impact Assessments and monitor their performance
- cooperate with, and act as the contact point for, the ICO
- act as a contact point for individuals on any issue relating to their data.

The DPO advises and monitors but does not make decisions on the Council's behalf and is not responsible for the Council's compliance. The Council will involve the DPO properly and in a timely manner, will not instruct the DPO on how to perform these tasks, and will ensure the DPO has no conflict of interest (Article 38).

5. Principles and lawful processing

5.1 The data protection principles

The Council will ensure that personal data is:

1. processed lawfully, fairly and transparently
2. collected for specified, explicit and legitimate purposes and not used in a way incompatible with those purposes
3. adequate, relevant and limited to what is necessary
4. accurate and, where necessary, kept up to date
5. kept no longer than necessary
6. kept secure, using appropriate technical and organisational measures.

The Council is responsible for, and must be able to demonstrate, compliance with these principles (accountability).

5.2 Lawful bases

Every processing activity must have a lawful basis under Article 6 UK-GDPR, recorded in the Record of Processing Activities. As a public authority, the Council will usually rely on:

Lawful basis	Typical Council examples
Public task (Art 6(1)(e)): exercising official authority or a task in the public interest	Correspondence and casework, consultations, planning responses, managing open spaces and facilities, CCTV
Legal obligation (Art 6(1)(c))	Payroll, tax and pension reporting, health and safety, statutory burial and allotment records, publishing councillor interests
Contract (Art 6(1)(b))	Employment, hall and facility hire, allotment tenancies, supplier contracts
Vital interests (Art 6(1)(d))	Emergencies where someone's life is at risk
Consent (Art 6(1)(a))	Optional activities only, such as newsletter mailing lists, publishing photographs of identifiable people, or volunteer contact lists

The Council will not rely on legitimate interests for processing carried out in performing its tasks as a public authority. Where consent is used, it must be freely given, specific, informed, unambiguous and recorded, and as easy to withdraw as to give. Consent will not be used where the Council would process the data anyway, or where there is a clear imbalance of power (for example, with employees).

5.3 Special category data

Special category data may only be processed where the Council also meets a condition under Article 9 UK-GDPR and, where required, Schedule 1 DPA 2018. Typical conditions are employment and social security obligations (for example, sickness absence and reasonable adjustments), substantial public interest conditions such as statutory and government purposes, and explicit consent where no other condition applies.

Where the Council relies on a Schedule 1 condition that requires it, it will maintain an Appropriate Policy Document. Access to special category data is restricted to those who need it.

5.4 Criminal offence data

Criminal offence data may only be processed under official authority or where a condition in Schedule 1 DPA 2018 applies (Article 10 UK-GDPR). Criminal record (DBS) checks will only be carried out where the role legally permits or requires them, and not on the basis of consent alone. CCTV images that may show offences are handled under section 7.2.

5.5 Purpose limitation and accuracy

Personal data collected for one purpose will not be used for an unrelated purpose unless the new purpose is compatible, required by law, or the individual has agreed. Staff and councillors should tell the Clerk promptly if their own details change. Where an individual disputes the accuracy of their data, the dispute will be recorded on file while it is considered.

6. Transparency and individuals' rights

6.1 Privacy Notices

The Council publishes Privacy Notices on its website and provides them when collecting personal data. They explain who the Council is, the DPO's contact details, the purposes and lawful bases for processing, who data is shared with, how long it is kept, individuals' rights, and the right to complain to the Council and to the ICO. Separate notices cover staff and councillors, and CCTV is signposted at the point of recording.

6.2 Individuals' rights

Individuals have the following rights, some of which depend on the lawful basis relied on:

Right	How it applies to the Council
To be informed	Met through Privacy Notices and CCTV signage
Access (subject access request)	A copy of their data and supporting information; see 6.3
Rectification	Inaccurate data corrected, incomplete data completed

Right	How it applies to the Council
Erasure	Applies in limited cases; usually not available where data is held to meet a legal obligation or perform a public task (Art 17(3))
Restriction	Processing paused, for example while accuracy is checked
Data portability	Only for data provided by the individual, processed by automated means on the basis of consent or contract
Object	Applies to public task processing; the Council must stop unless it has compelling legitimate grounds; always applies to direct marketing
Automated decision-making	The Council does not make decisions with legal or similarly significant effects by solely automated means

Where data has been rectified, erased or restricted, the Council will tell any recipients it was disclosed to, unless that is impossible or involves disproportionate effort (Article 19).

6.3 Handling requests

Requests may be made verbally or in writing, to any councillor or member of staff, and need not mention data protection law. Anyone who receives one must pass it to the Clerk the same day. The Clerk will log it and consult the DPO as needed.

- Requests are answered without undue delay and within one month of receipt. This may be extended by up to two further months for complex or numerous requests, with the individual told within the first month.
- The time limit does not start until the Council has any identity verification it reasonably needs, and may be paused while the Council waits for clarification it reasonably needs to respond.
- For subject access, the Council will carry out reasonable and proportionate searches.
- No fee is charged, unless a request is manifestly unfounded or excessive, in which case the Council may charge a reasonable fee or refuse, giving reasons.
- Third-party information and other exempt information will be redacted or withheld where the law allows, with the reasons recorded.

6.4 Data protection complaints

Individuals may complain to the Council if they believe their personal data has been handled in breach of data protection law. Under section 164A DPA 2018, the Council operates a Data Protection Complaints Procedure under which it will:

- accept complaints however submitted, and offer an electronic means of making them (for example, an online form or email)

- acknowledge each complaint within 30 days of receipt
- take appropriate steps without undue delay to respond, including making enquiries and keeping the complainant informed
- tell the complainant the outcome without undue delay.

Individuals also have the right to complain to the ICO (ico.org.uk, 0303 123 1113), and will be told this in Privacy Notices and in responses to rights requests.

6.5 Electronic communications

The Council will only send electronic newsletters or promotional messages to people who have actively opted in and will honour any request to stop. Service messages (for example, about a booking or allotment tenancy) are not marketing.

7. Keeping personal data secure

7.1 Security measures

The Council will protect personal data against unauthorised access, loss, damage and misuse. Councillors, staff and volunteers must:

- use long, unique passwords or passphrases for every Council account, ideally stored in a reputable password manager, and enable multi-factor authentication wherever it is available
- change a password straight away if it may have been compromised (routine forced changes are not required)
- lock screens when away from a device, and keep devices updated with security patches and anti-malware protection
- protect laptops, tablets and phones used for Council business with a PIN or password and device encryption
- store Council files in the Council's approved systems, not on personal cloud accounts, removable media or personal email
- use removable media (such as USB sticks) only where unavoidable, encrypted, and never as the only copy
- keep paper records in locked storage, operate a clear desk, and shred or use confidential waste when records are no longer needed
- take care to address emails correctly and use BCC for group emails to members of the public.

The Clerk will ensure Council data is regularly backed up, that access permissions are reviewed when people join or leave, and that leavers return or securely delete Council information.

7.2 CCTV

The Council operates CCTV at the Horsmonden public conveniences to prevent and detect crime and anti-social behaviour, under its CCTV Policy and Data Protection Impact Assessment. Signage is displayed at the site. Recordings are stored securely, overwritten automatically after 30 days unless required for an investigation, and viewed only by the Clerk or Deputy Clerk when necessary. Footage may be disclosed to the police or other authorised bodies where lawful, and each disclosure is logged.

7.3 Retention and disposal

Personal data will be kept only for as long as necessary for the purpose it was collected, in line with the Council's Retention Schedule. At the end of the retention period, it will be securely destroyed or deleted. The Retention Schedule is reviewed alongside this policy.

7.4 Processors and sharing

Where a third-party processes personal data on the Council's behalf, the Council will check before appointment that it provides sufficient guarantees of security and compliance, and will put a written contract in place meeting Article 28 UK-GDPR. The DPO's advice should be sought on new suppliers that handle personal data.

Personal data will only be shared with other organisations where there is a lawful basis and it is necessary, for example with HMRC and the pension provider, with the police where lawful, or where required by law. Regular sharing will be documented and covered by a data sharing agreement where appropriate.

7.5 International transfers

Personal data will not be transferred outside the UK unless the transfer is covered by adequacy regulations or appropriate safeguards (such as the UK International Data Transfer Agreement or Addendum). This includes data held by cloud and email providers, which the Clerk will check when assessing a service.

7.6 Data protection by design and Data Protection Impact Assessments

The Council will build data protection into new projects, systems and services from the outset, and will set the most privacy-friendly options by default. A Data Protection Impact Assessment (DPIA) will be completed before any processing likely to result in a high risk to individuals, such as new or extended CCTV, new technology, or large-scale processing of special category data. The Council (through the Clerk) carries out the DPIA, seeking the DPO's advice (Article 35), and the outcome is recorded.

7.7 Record of Processing Activities

The Clerk maintains a Record of Processing Activities (data register) describing what personal data is held, why, the lawful basis, where it is stored, who it is shared with and how long it is kept. It is reviewed at least annually and whenever processing changes.

7.8 Personal data breaches

Anyone who discovers or suspects a personal data breach (for example, an email sent to the wrong person, a lost device or paperwork, or unauthorised access to an account) must report it to the Clerk immediately, and in any event the same day. The Clerk will follow the Data Breach Procedure, consulting the DPO, to:

- contain the breach and recover data where possible
- assess the risk to the individuals affected
- notify the ICO within 72 hours of becoming aware, unless the breach is unlikely to result in a risk to individuals' rights and freedoms

- tell affected individuals without undue delay where the breach is likely to result in a high risk to them
- record every breach, whether or not reported, with its effects and the action taken, in the breach log.

8. Training

All councillors, employees and regular volunteers who handle personal data will receive data protection training on joining (as part of induction for staff, and within three months of election or co-option for councillors) and refresher training at least annually, or sooner if the law or the Council's procedures change significantly. Training will cover this policy, recognising and handling rights requests and complaints, security, and breach reporting. The Clerk will keep a record of training completed. Training is compulsory.

9. Monitoring and review

The Clerk will monitor day-to-day compliance with this policy. The DPO will monitor compliance independently, including through periodic review and audit, and will report findings and recommendations to the Council. This policy will be reviewed annually whenever there is a significant change in the law or the Council's processing.

10. Compliance with this policy

The Council takes compliance with this policy seriously. A breach of this policy may expose individuals to harm and the Council to regulatory action, and in some cases may be a criminal offence (for example, knowingly or recklessly obtaining or disclosing personal data without the Council's consent, under section 170 DPA 2018).

- For employees, a breach may lead to action under the Council's disciplinary procedure, which may result in dismissal.
- For councillors, a breach may be referred as a potential breach of the Members' Code of Conduct.
- For volunteers and contractors, a breach may lead to the end of the arrangement.

Anyone with questions about this policy should contact the Clerk or the DPO.

Approval

Adopted by	Date	Minute reference	Next review
Horsmonden Parish Council	[date]	[ref]	[date + 12 months]