



How to Make a Data Access Request

Under the UK General Data Protection Regulation (UK GDPR), individuals have the right to request access to personal data held about them by Hullbridge Parish Council. This is known as a **Subject Access Request (SAR)**.

To make a request, please write to the **Clerk to the Council** using the contact details provided on the Council's website or in official correspondence. Your request should include:

- Your full name and contact details.
- A clear description of the information you are requesting.
- Any details that may assist the Council in identifying the data (such as dates, locations, or context of the interaction).
- Proof of your identity and, where relevant, proof of authority to act on behalf of someone else.

Requests may be submitted by **email or post**. The Council will acknowledge your request and normally respond within **20 working days** from receipt of all the necessary information and identification. In accordance with Article 12(3) of UK GDPR, this period may be extended by a further two months if the request is complex or numerous. If this is the case, the Council will inform you within the initial one-month period and explain the reasons for the delay.

There is **no fee** for submitting a Subject Access Request. However, a **reasonable fee** may be charged for:

- Repetitive or excessive requests;
- Requests for additional copies of previously provided data;
- Requests that are manifestly unfounded.

All SARs and responses are logged in accordance with the Council's **Record of Processing Activities (ROPA)** and **Information Asset Register**, and handled securely and confidentially.

If you are dissatisfied with how your request has been handled, you have the right to lodge a complaint with the **Information Commissioner's Office (ICO)** via www.ico.org.uk or by calling 0303 123 1113.

Data protection impact assessments

template for carrying out a data
protection impact assessment on
surveillance camera systems



Project name: CCTV in the Parish of Hullbridge

Data controller(s): Hullbridge Parish Council

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA¹:

- | | |
|---|---|
| <input type="checkbox"/> Systematic & extensive profiling | <input type="checkbox"/> Large scale use of sensitive data |
| <input checked="" type="checkbox"/> Public monitoring | <input type="checkbox"/> Innovative technology |
| <input type="checkbox"/> Denial of service | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Data matching | <input type="checkbox"/> Invisible processing |
| <input type="checkbox"/> Tracking | <input type="checkbox"/> Targeting children / vulnerable adults |
| <input type="checkbox"/> Risk of harm | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making | <input type="checkbox"/> Other (please specify) |

CCTV in Pooles Lane Car Park initially installed in 2015 new installation April 2025/ CCTV at Parish Office 98 Ferry Road and forecourt in place since 2015.

We are processing under the Data Protection Act 2018 and UK GDPR.

2. What are the timescales and status of your surveillance camera deployment? Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

All cameras and equipment have been approved by Full Council

There are no current plans for additional CCTV. If new cameras are installed we will continue to process data under the Data Protection Act 2018.

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?

Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

There are 10 cameras situated at Pooles Lane Car Park and 4 cameras at Parish Office 98 Ferry Road.

The cameras are to provide a safe and secure environment for residents and visitors, to deter crime and anti social behaviour, to assist law enforcement and to act as a visible deterrent.

¹ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/>

There have been a number of reported incidents in the areas where the cameras are situated in particular with relation to car crime and anti social behaviour.

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

The council will be processing members of the public personal data who use Pooles Lane Car Park , and who enter or approach the Parish Office at 98 Ferry Road. The images will be kept for a maximum period of 30 days.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

Hullbridge Parish Council will be making decisions about the uses of the system. The system operatives will be the Parish Clerk and Maintenance Officer, and the parish council's appointed security firm who will have the appropriate licences in place. The data will only be disclosed to the authorised agencies when requested for the purposes of evidencing crime or supporting their activities in searching for individuals. Individuals can request a copy of CCTV data which contains their personal data. Authorisation for this will require agreement by both the Clerk and Chair of the Council.

6. How is information collected? (tick multiple options if necessary)

- | | |
|--|---|
| <input checked="" type="checkbox"/> Fixed CCTV (networked) | <input type="checkbox"/> Body Worn Video |
| <input type="checkbox"/> ANPR | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras | <input type="checkbox"/> Redeployable CCTV |
| <input type="checkbox"/> Other (please specify) | |

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

Camera feed is recorded automatically on to a hard disk, this recording can be accessed remotely from the Parish Office. A live feed can be viewed via a mobile app (restricted to Parish mobile devices) All recordings are overwritten every 30 days.

8. Does the system's technology enable recording?

☒ Yes ☐ No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

Recording undertaken at Pooles Lane Car park in a locked storage room / recording undertaken in the Parish Office 98 Ferry Road in a locked cabinet in an office which is locked and alarmed when not occupied by Parish staff. I

9. If data is being disclosed, how will this be done?

- ☒ Only by on-site visiting
☒ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)
☒ Off-site from remote server
☐ Other (please specify)

Copies of footage will be released to either an individual who has requested a copy of their personal data or to authorised agencies to aid the evidence of a crime/find individuals. The images will be downloaded onto a memory stick and collected in person.

10. How is the information used? (tick multiple options if necessary)

- ☐ Monitored in real time to detect and respond to unlawful activities
- ☐ Monitored in real time to track suspicious persons/activity
- ☐ Compared with reference data of persons of interest through processing of biometric data, such as facial recognition.
- ☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software
- ☐ Linked to sensor technology
- ☒ Used to search for vulnerable persons
- ☒ Used to search for wanted persons
- ☒ Recorded data disclosed to authorised agencies to support post incident investigation, including law enforcement agencies
- ☒ Recorded data disclosed to authorised agencies to provide intelligence
- ☒ Other (please specify)

Upon request by an individual for their personal data.

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken
Residents	Parish Meeting	concerns about anti-social behaviour and car crime	Upgraded CCTV system installed at Pooles Lane Car Park
Parish Staff	Team meeting	concerns about office / van security	CCTV in place at parish office / upgrade to be budgeted for
Residents	Parish Meeting	High street safety and car crime	To initiate discussions and budget for future high street rollout of CCTV

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

Under section 17 of the Crime and Disorder Act 1988 a local council has a duty to: exercise its various functions with regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent,

- crime and disorder in its area (including anti social behaviour and other behaviour adversely affecting the local environment
- misuse of drugs, alcohol and other substances in its area and;
- re- offending in its area

In addition Section 31 of the Local Government and Rating Act 1997 permits a local council, in order to prevent or detect crime to:

- install and maintain equipment
- establish and maintain any scheme, or
- assist others to install and maintain any equipment or to establish and maintain any scheme

The Law Enforcement Directive (LED) enables the Council to process personal information without some of the normal safeguards required by the General Data Protection Regulations. LED controls the processing of personal data where it relates to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to public security. The Council also uses CCTV camera systems under Section 163 Criminal Justice and Public Order Act 1994.

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

Signage is clearly visible with relevant contact information in all areas monitored by CCTV.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

The cameras run 24/7 and will record all activities occurring within their viewing capacity. The viewing of this data will only occur when requested by appropriate authorised authorities.

Benefits will be measured by the reduction of reported incidents

By engaging with residents at council meetings and surgeries we can ensure they feel safer in the local environment.

15. How long is data stored? (please state and explain the retention period)

30 days - the system will overwrite data recorded after 30 days. This is considered long enough for any approved authorities to contact the council for footage to support any crimes.

16. Retention Procedure

- ☒ Data automatically deleted after retention period
- ☐ System operator required to initiate deletion
- ☐ Under certain circumstances authorised persons may override the retention period, e.g. retained for prosecution agency (please explain your procedure)

If the police or relevant agencies require footage it will be sent via an encrypted channel or downloaded to a memory stick which will be kept in a locked cabinet prior to collection.

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The system is situated in a lockable offices with keys any available to parish staff. Any downloaded recordings will be password protected and locked away until collection. Any persons collecting recordings will have to be authorised and prove identity, any data downloads and collections will be recorded by the Clerk.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

The council recognises that individuals whose information is recorded have a right to be provided with that information, or if they consent to it, view that information. Requests will be dealt with promptly. It should be noted that individuals will have a maximum of 30 days to make a request before footage is automatically deleted. All requests are subject to operational considerations e.g;

- Footage has been requested by and/or passed to the Police as part of an investigation of a crime; or
- Footage has been requested in respect of a road traffic collision and the information has been passed to insurers; or
- Any relevant exemptions. The individual will be asked to supply current photographic evidence of identity, and approximate timings of recorded events to assist with viewing.

19. What other less intrusive solutions have been considered? You need to consider other options prior to any decision to use surveillance camera systems. For example, could better lighting or improved physical security measures adequately mitigate the risk? Does the camera operation need to be continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

The other effective method to deter crime is an active police presence , but at this time of reduced service in the local area this is not a realistic alternative. The council employ a security firm to assist with public safety, but most reported incidents occur outside of any patrols.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

- ☒ The agencies that are granted access
- ☒ How information is disclosed
- ☒ How information is handled

Are these procedures made public? ☒ Yes ☐ No

Are there auditing mechanisms? ☒ Yes ☐ No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

The CCTV policy has been updated after the new installation and is reviewed annually by the council this is available for public view on the council website. An internal auditor reviews processes and policies on an annual basis of which this is included. The CCTV provider provides maintenance and verifies and upgrades the system as required.

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, how long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Intrusions into the privacy of residents	Remote, possible or probable Possible	Minimal, significant or severe significant	Low, medium or high Medium
Share data with incorrect 3 rd party	possible	minimal	Low
Access by unauthorised parties	Remote	Severe	Low
Non automatic deletion of recorded data	Remote	Minimal	Low

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Tampering or removal of signage	Remote, possible or probable Possible	Minimal, significant or severe Minimal	Low, medium or high Low
Vandalism	Possible	Minimal	Medium
Sharing of recording - the CCTV policy and procedures mitigate the risk of inappropriately sharing recordings	Remote	Minimal	Low

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Cameras are positioned to avoid any intrusion into private space and only record public areas. It is reasonable to expect that CCTV will record individuals in public areas.	Eliminated reduced accepted Eliminated	Low medium high Low	Yes/no Yes
Data will only be shared to specific authorised agencies as set out in this assessment	Reduced	Low	Yes
AML Security and MPE Alarm are the installing companies . They have robust security and access protection which has been approved by the council	Reduced	Low	Yes

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
The system has been tested for automatic deletion and will form part of regular checks so ensure that no data greater than 30 days is available	Eliminated reduced accepted Eliminated	Low medium high Low	Yes/no Yes
Visual checks of the signage will be regularly carried out, with spare signs available to replace should this be necessary.	Reduced	Low	Yes
Cameras are not easily accessible and therefore are at reduced risk of vandalism.	Reduced	Low	Yes
Data only to be available to approved personnel and kept in locked areas/ and or password protected.	Eliminated	Low	Yes

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. [Further information](#) is on the ICO website.

Item	Name/date	Notes
Measures approved by: Hullbridge Parish Council	2025	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by: N/A		If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images.
DPO advice provided by:	Not applicable as parish councils are not obliged to have Data Protection Officers (DPO'S)	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice Not applicable as parish councils are not obliged to have Data Protection Officers (DPO'S)		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.

Comments:

This DPIA will be kept
under review by:

The DPO should also review
ongoing compliance with DPIA.

APPENDIX ONE

This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Parish Office	1	4	24hrs	Not monitored	Cameras are installed here to respond to high crime trends, deal with the fear of crime
Public car park		10	24hrs	Only Monitored if a crime is reported	Cameras are installed here to respond to high crime trends, deal with the fear of crime

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:

		Camera Types (low number low impact – High number, High Impact)									
Location Types A (low impact) Z (high impact)											

NOTES



Hullbridge Parish Council

CCTV Policy

Adopted ??

Introduction

This policy sets out the management, operation, and confidentiality arrangements for the Closed-Circuit Television (CCTV) systems located at:

- The Parish Office 98 Ferry Road SS5 6EX
- Pooles Lane Car Park Ferry Road SS5 6ND

Both CCTV systems are managed by Hullbridge Parish Council in accordance with current data protection legislation.

The policy was prepared inline with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and guidance issued by the Information Commissioners Office (ICO). It will be reviewed annually to ensure continued compliance and relevance.

The Council is registered with the Information Commissioner under Registration Reference: Z6496438.

Purpose of CCTV System

- Provide a safe and secure environment for residents, visitors, and those working in the are.
- Prevent, deter and detect crime and disorder, including fly-tipping and anti-social behaviour.
- Assist law enforcement and other authorised agencies in the investigation and prosecution of criminal offences.
- Act as a visible deterrent through the clear siting of cameras and appropriate signage.

Data Protection Principles

In accordance with UK GDPR, all CCTV data will be:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Retained only for as long as necessary.
- Processed securely and in a way that protects against unauthorised access, loss or damage.
- Managed in accordance with the rights of individuals.



A Data Protection Impact Assessment (DPIA) has been completed for the CCTV system.

Signage

Clear signage is displayed in all areas covered by CCTV to inform individuals that surveillance is in operation. The signs include:

- The purpose of the CCTV.
- The name of the data controller (Hullbridge Parish Council).
- Contact details for further information.

Retention and Storage

CCTV images are retained for a maximum of 30 days unless required for a specific investigation or legal proceedings. All recordings are securely stored and access is restricted to authorised personnel only.

Access to CCTV Images

Access to recorded images is limited to the Clerk to the Parish Council, authorised operators, and law enforcement agencies.

Access will only be granted for lawful reasons including:

- Crime investigation or prevention.
- Legal or insurance matters.
- Responding to subject access requests.

All access and disclosures are recorded in an access log.

Subject Access Requests

Individuals have the right to request access to CCTV footage in which they appear. Requests must:

- Be made in writing to the Parish Clerk.
- Include sufficient information to identify the individual and the date/time of the footage.
- Provide proof of identity.

Disclosure may be limited or refused if it would involve disclosing images of other individuals or interfere with an ongoing investigation.



Operation and Management

Day-to-day operational responsibility rests with the Clerk to the Parish Council. All personnel and contractors operating or managing the CCTV system will be trained in its lawful and appropriate use.

Operators must:

- Act with integrity and not abuse the system.
- Avoid compromising the privacy of individuals.
- Ensure date/time settings on the system are accurate.
- Record and justify any access to or use of recorded images.

The CCTV system's performance and compliance will be reviewed annually by the Parish Council.

Third-Party Access and Security Firm Requirements

Law Enforcement Agencies and the Parish Council's appointed security contractor may access footage where lawful and necessary.

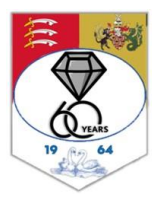
The appointed security firm must hold the appropriate licences and accreditations required by law to carry out CCTV monitoring and related security functions. This includes, but is not limited to, licences issued by the Security Industry Authority (SIA). Proof of valid licensing must be provided prior to the commencement of services and maintained throughout the contract.

Complaints and Concerns

Any concerns or complaints about the operation of the CCTV system should be submitted in writing to the Parish Clerk. Complaints will be considered in accordance with the Parish Council's existing Complaints Policy.

Contact:

Hullbridge Parish Council
98 Ferry Road, Hullbridge, SS5 6EX
clerk@hullbridge-pc.gov.uk | 01702 232038



Data Audits and Ongoing Compliance

Adopted ?? – Reviewed Annually

In line with the 2025 guidance from the Smaller Authorities Proper Practices Panel (SAPPP), Hullbridge Parish Council will conduct regular data audits as part of its commitment to maintaining the highest standards of data protection.

Purpose of Data Audits:

The purpose of data audits is to:

- Identify all personal data held by the Parish Council.
- Review how this data is collected, stored, accessed, shared, and disposed of.
- Ensure all data processing activities are lawful, necessary, and proportionate.
- Confirm compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, and local authority best practices.

Frequency:

Data audits will be carried out annually, and additionally:

- When there are significant changes to systems or services.
- Following any data breach or incident.
- As part of onboarding or offboarding major contracts or services involving personal data.

Process:

1. Data Mapping Update: Review and update the existing Data Mapping document to reflect all personal data processed.
2. Risk Assessment: Identify risks associated with each data type, including data security, access controls, and third-party processing.
3. Audit Log: Maintain an audit log summarizing findings, required actions, and improvements made.
4. Reporting: Present audit results to the Council and record in meeting minutes where appropriate.

Responsibilities:

The Clerk, in their capacity as the Data Protection lead, is responsible for ensuring that:

- The audit is carried out effectively.
- Any compliance issues identified are addressed promptly.
- Training is provided where necessary to staff and Councillors.

Review:

The Data Protection Policy, including the audit process, will be reviewed annually or in response to changes in legislation or data processing practices.



Hullbridge Parish Council Data Protection Policy

Adopted ?? – Reviewed Annually

1. Purpose

Hullbridge Parish Council is committed to protecting the rights and privacy of individuals in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This policy sets out our approach to data protection and outlines the rights and obligations of individuals whose personal data we process, including staff, councillors, volunteers, contractors, and residents.

This policy supports and aligns with the Council's Information Asset Register and Record of Processing Activities (ROPA), and General Privacy Notice which record and monitor all data processing activities undertaken by the Council.

2. Definitions

- Personal Data: Any information relating to an identified or identifiable natural person.
- Special Category Data: Includes data on racial or ethnic origin, political opinions, religious beliefs, health, sexual orientation, and trade union membership.
- Processing: Any operation performed on personal data, including collection, storage, use, disclosure, or destruction.
- Data Controller: Hullbridge Parish Council, who determines the purposes and means of processing.
- Data Processor: Any party processing data on behalf of the Council.
- Data Subject: An individual whose personal data is processed.
- Data Protection Officer: While not required by law for parish councils, the Council has designated a Data Protection Lead (Clerk to the Council) responsible for compliance.

3. Data Protection Principles

The Council is committed to the principles of data protection as defined in Article 5 of UK GDPR. 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.

4. Lawful Basis for Processing

Personal data will be processed by the Council under one or more of the following legal bases:

- Consent of the data subject.
- Contractual necessity.
- Legal obligation.
- Vital interests.
- Public task (most common for council activities).
- Legitimate interests (only in very limited contexts).

Special category data will only be processed where a lawful condition under Article 9 of UK GDPR is met, such as employment rights, legal claims, or public interest.

All processing activities are recorded in the Council's ROPA, including the legal basis, data categories, retention periods, and security measures.

5. Data Subjects' Rights

Individuals have the following rights under UK GDPR:

- Right to be informed (via Privacy Notices).
- Right of access (Subject Access Request).
- Right to rectification.
- Right to erasure (in limited circumstances).
- Right to restrict processing.
- Right to data portability (where applicable).
- Right to object.
- Rights related to automated decision-making (not used by the Council).

Requests must be made to the Clerk and will be responded to within one month, subject to verification of identity.

6. Data Security

Hullbridge Parish Council maintains appropriate technical and organisational measures to ensure the security and confidentiality of all personal data. This includes:



- Access control (physical and digital).
- Use of encrypted devices and secure passwords.
- Training for councillors, staff and volunteers.
- Regular review of processing activities and associated risks.

Details of asset-level security controls are documented in the Information Asset Register.

7. Data Breaches

All data breaches will be investigated. If a breach is likely to result in a risk to individuals' rights and freedoms, the Information Commissioner's Office (ICO) will be notified within 72 hours.

Where required, affected data subjects will also be informed without undue delay.

All breaches and near-misses are logged and reviewed.

8. Data Sharing & Processors

Where the Council shares data with third parties (e.g. payroll providers, contractors), this will be done under a written agreement ensuring compliance with UK GDPR.

Third parties acting as data processors must provide sufficient guarantees to implement appropriate safeguards.

9. Data Protection Impact Assessments (DPIAs)

A DPIA will be conducted for any high-risk processing activity, such as the use of CCTV or large-scale data collection. DPIAs will assess risks and identify mitigation measures.

10. Data Retention & Disposal

The Council follows a documented Retention Schedule, which defines how long data is held. This schedule is integrated into the ROPA and Information Asset Register.

Data is securely destroyed when no longer required.

11. Roles and Responsibilities

- Clerk to the Council: Acts as the Data Protection Lead.
- All staff and councillors: Must comply with this policy and attend training as



required.

- Volunteers and contractors: Must be briefed on data protection responsibilities.

12. Training

All councillors, staff, and volunteers are trained on data protection principles and responsibilities on induction and annually thereafter.

Specialist training is provided to those handling sensitive data or responding to subject access requests.

13. Review and Monitoring

This policy will be reviewed annually or in response to changes in legislation, guidance from the ICO, or significant changes to Council operations.

14. How to Make a Data Access Request

Individuals have the right to access the personal data that Hullbridge Parish Council holds about them. This is known as a Subject Access Request (SAR).

To make a Subject Access Request, you should submit a written request to the Clerk to the Council. Your request should include:

- Your full name and contact details.
- A clear description of the information you are requesting.
- Any details that will help the Council locate the information (e.g., relevant dates, interactions, or services).
- Proof of your identity (such as a copy of a passport or driving licence and a utility bill showing your current address).

Requests can be submitted by email or post. The Council will acknowledge receipt and respond within 20 working days of receiving all necessary information. If the request is complex or involves numerous records, this deadline may be extended, and you will be notified within the original time frame. There is no charge for making a request. However, the Council may charge a reasonable fee if the request is manifestly unfounded or excessive, or if additional copies of the information are requested.

If you are unhappy with the Council's handling of your request, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk.



General Privacy Notice

Hullbridge Parish Council

Hullbridge Parish Council is committed to protecting your privacy and personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We are a Data Controller registered with the Information Commissioner's Office (ICO) – Registration No. Z6496438.

1. Why We Collect Your Data

We collect and process personal data to:

- Deliver our statutory functions and local services
- Respond to enquiries, complaints, or requests
- Manage allotments, events, grants, and public consultations
- Support community safety (e.g., CCTV, emergency planning)
- Meet legal obligations (e.g., employment, finance, public health)

2. What Data We Collect

Depending on your interaction with us, we may collect:

- Names, addresses, contact details
- Email correspondence
- CCTV footage
- Age, gender, or equalities data
- Financial details (e.g., for grants or payroll)
- Correspondence through email, post, telephone or social media

We process data under the following legislation:

- Local Government Act 1972
- Localism Act 2011
- Freedom of Information Act 2000
- Environmental Information Regulations 2004



HULLBRIDGE PARISH COUNCIL

- Health and Safety at Work etc. Act 1974
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

3. Legal Basis for Processing

We process personal data:

- To carry out tasks in the public interest or under a legal obligation
- With your consent (e.g., email mailing lists)
- Under a contract (e.g., employment)
- Occasionally, in the vital interests of individuals (e.g., emergencies)

4. Data Sharing

We only share your information when necessary:

- With trusted service providers under contract
- With government authorities (e.g., HMRC, Police, DWP) if required by law
- With emergency services during incidents

We do not share your data for marketing purposes without consent.

5. Data Retention

We keep personal data only for as long as necessary. Our full retention schedule is available in the Council's Retention Policy. Some information is kept permanently for archiving and historical purposes.

6. Security

We use appropriate technical and organisational measures including:

- Password-protected systems
- Secure locked storage for paper records
- Encrypted backups and restricted access to data

7. Your Rights

Under UK GDPR, you have rights to:

- Access your data
- Request correction or deletion



HULLBRIDGE PARISH COUNCIL

- Restrict or object to processing
- Lodge a complaint with the ICO

For full details, visit: <https://ico.org.uk>

8. CCTV and Social Media

Images captured on CCTV are used for public safety and crime prevention. Footage is retained for 30 days unless required longer for investigations. Visit our CCTV policy for more information.

We also process personal data via our Facebook page and website in line with this notice.


9. Contact Us

For questions or to exercise your rights, contact:

Clerk to Hullbridge Parish Council

98 Ferry Road, Hullbridge, Essex SS5 6EX

 Email: clerk@hullbridge-pc.gov.uk

 Phone: 01702 232038

10. Changes to This Notice

This privacy notice is reviewed regularly and was last updated on 8th September 2025. It replaces the previous version adopted on 9 April 2018.