LENHAM
PARISH COUNCIL

Controlled Document

Title	Data Protection Policy
Author	Lenham Parish Council
Owner	Lenham Parish Council
Subject	Main Policy Documents
Government Security Classification	Official
Document Version	Version 1
Created	26.08.2025
Approved By	Full Council
Review Date	October 2027

Version Control

Version	Date	Author	Description of Change	Sign
1	**1.10.2025**	**Lenham Parish Council**	**Original Policy**	**L.Westcott**

Data Protection Policy

Purpose

Lenham Parish Council (LPC) is fully committed to compliance with the requirements of the General Data Protection Regulation 2016/679 (UK GDPR) and the Data Protection Act 2018 (DPA). LPC will, therefore, follow procedures which aim to ensure that all personal data collected about council members, staff, visitors and other individuals processed fairly, lawfully and transparently.

The UK GDPR, the DPA and Article 8 of the Human Rights Act 1998, stress that the processing of personal data needs to strike a balance between the needs of the LPC to function effectively and respect the rights and freedoms of the individual. This policy sets out how LPC intends to safeguard those rights and freedoms.

Obligations and responsibilities under the UK GDPR are not optional; **they are mandatory.**

LPC therefore, follow procedures that aim to ensure that all members of staff, visitors and any other person working for LPC will have access to any personal data held by or on behalf of LPC is fully aware of, and abides by their duties and responsibilities under UK GDPR and DPA.

All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the role being undertaken.

As well as LPC, any individual who knowingly or recklessly processes data without appropriate consent or proper authorisation, for purposes other than those for which it is intended or is deliberately acting outside of their recognised responsibilities may be subject to Parish Council's disciplinary procedures, including dismissal where appropriate and possible criminal conviction under the DPA 2018

This policy relates to the collection and processing of all personal data held by LPC, falling within the scope of the UK GDPR and DPA in all formats and any data processed on behalf of LPC including paper, electronic, audio and visual. It applies to all members, staff, volunteers, agents or by third parties and contractors.

Personal and special category personal data.

The UK GDPR and DPA provide conditions for the collection and processing of any personal data. It also makes distinction between **Personal data and special category personal data.**

Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade union membership
- Physical or mental health conditions
- Sexual life or sexual orientation
- Genetics
- Biometric data

Although there are clear distinctions between personal and special category data for the purpose of this policy the term 'personal data' refers equally to 'special category data' unless otherwise stated.

The UK GDPR and DPA rules for special category data do not apply to information about criminal allegations proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions, or related security measures.

Personal data processed by Lenham Parish Council

LPC processes personal data for a variety of Council purpose about our employees, residents, suppliers and other individuals. A description of the types of personal data processed and the purposes for processing are included in the Parish Council privacy notices. See LPC website for full notices and updates.

Personal data must be handled and dealt with in accordance with the UK GDPR and DPA and this policy. There are safeguards within the UK GDPR and DPA to ensure personal information is collected, recorded and used whether it is paper, computer records or recorded by any other means.

The obligations outlined in this policy apply to everyone who has access to, holds copies of or processes personal data. This includes those who work from /at home or have remote or flexible working patterns.

The Data Controller

LPC is the Data Controller for all personal data it holds. The Parish Clerk has day-to-day responsibility for ensuring compliance with data protection legislation on behalf of the Council.

Roles and Responsibilities

The Parish Council
LPC is responsible for ensuring that personal data is processed in accordance with the principles of the UK GDPR and the Data Protection Act 2018.

The Data Protection Officer (DPO)

In accordance with Article 37 of the UK GDPR, LPC has appointed the Parish Clerk as its Data Protection Officer. The DPO operates independently but reports to Full Council and there role is to:

- Inform and advise the Council and its staff about their obligations under data protection law,
- Monitor compliance with the Council's data protection policies and procedures,
- Provide advice on Data Protection Impact Assessments (DPIAs),
- Cooperate with the Information Commissioner's Office (ICO) and act as the Council's contact point.

The DPO carries out these tasks independently, reporting to Full Council where required.

All Staff and Councillors

All staff and councillors are responsible for:

a. Collecting, storing and processing any personal data in accordance with this policy,
b. Informing the Clerk of any changes to their personal data, such as a change of address,
c. Contacting the Clerk in the following circumstances:
    i. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    ii. If you have any concerns that this policy is not being followed.
    iii. If you are unsure whether or not you have a lawful basis to use personal data in a particular way.
    iv. If you need to reply on or capture consent, deal with the rights of the data subject or transfer personal data outside the European Economic Area.
    v. If there has been a data breach.
    vi. Whether you are engaging in a new activity that may affect the privacy of individuals.
    vii. If you need help with any contracts or sharing personal data with third parties

Data Protection Principles

Anyone processing personal data must comply with the principles of good practice. These principles are legally enforceable and can be summarised as follows:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals;
b. Obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
d. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;
e. Kept in a form which permits identification of data subjects for no longer than is necessary

for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose subject to implementation of the appropriate technical and organizational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals;

f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. In accordance with the rights of data subjects under the UK GDPR and DPA.

Lawful Bases for Processing

LPC will only process personal data where it has a lawful basis to do so under the UK GDPR and the Data Protection Act 2018. The lawful bases are:

a. Consent – the individual has given clear consent for LPC to process their personal data for a specific purpose;
b. Contract – the processing is necessary for a contract with the individual, or because they have asked LPC to take specific steps before entering into a contract.
c. Legal obligation – the processing is necessary for LPC to comply with the law;
d. Vital interests – the processing is necessary to protect someone's life;
e. Public task – the processing is necessary for LPC to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law;
f. Legitimate interests – the processing is necessary for LPC's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This basis is less commonly relied upon by public authorities acting in their official capacity.)

When processing special category data or criminal offence data, LPC will ensure that an additional lawful condition under Articles 9 or 10 UK GDPR is also met.

Fair Processing

In meeting any obligation to ensure that processing of information is fair, due consideration will be given to the adoption of any recognised standards or advice to provide individuals with such information as it necessary to ensure that they are likely to understand:-

a. The purposes for which their personal data are to be processed;
b. The likely consequences of such processing and;
c. Whether particular disclosures can be reasonably envisaged

Notification

The national body for the supervision of UK GDPR is the Information Commissioners Office (ICO) to whom the Clerk notifies their purposes for processing personal data.

This notification process serves to provide transparency and openness about the processing of personal data. It is fundamental principles of the UK GDPR that the public should know or be able to find out who is carrying out the processing of personal data and for what purposes.

LPC is registered with the Information Commissioner's Office (ICO) and pays the annual data protection fee. The registration number is ZB528442.

Individuals Rights

LPC recognises that access to personal data held about an individual is a fundamental right provided in the DPA. These rights include :-

a. The right to be informed,
b. The right of access to personal data,
c. The right to request rectification,
d. The right to request erasure,
e. The right to restrict processing in certain circumstances,
f. The right to data portability,
g. The right to object to processing,
h. Rights related to automated processing decision-making including profiling.

LPC will ensure that all requests from individuals to access their information is responded to within one calendar month which is the time allowed in legislation. However the one month timescales will not commence until after receipt of proof of identity or clarification of information sought. To minimise delays and unnecessary work all data requested must:

a. Be made in writing (paper or email) to clerk@lenhamparishcouncil.org.uk
b. Be accompanied by adequate proof of the identity of the data subject where required and, where applicable, the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative, or, authorised agent).
c. Specify clearly and simply the information required.
d. Give adequate information to enable the requested data to be located.
e. Make it clear where the response should be sent.

The Clerk must be informed of any request to take action against one or more of these rights.

The DPA allows exemption from providing information to individuals making a subject access request, and non-disclosure of information, in specific and limited circumstances.

When LPC collect personal data, it does not need to provide the individual with any information they may already have.

When obtaining personal data from other sources, LPC do not need to provide individuals with privacy information if:

a. The individual already has the information;
b. Providing the information to the individual would be impossible,
c. Providing the information to the individual would involve disproportionate effort;
d. Providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
e. LPC is required by law to obtain or disclose the personal data; or
f. LPC is subject to an obligation of professional secrecy regulated by law that covers personal data.

If a data subject remains dissatisfied with a response received, they may ask for the matter to be reviewed, or, in the case of an employee a solution may be sought using the LPC grievance process.

Ultimately, if a data subject continues to be dissatisfied they have the right to ask the Information Commissioners Office (ICO) to carry out an assessment of their case and / or pursue a legal remedy under DUAA 2025.

Legal Requirements

LPC may be required to disclose personal data by a court order, or the comply with other legal requirements including the prevention or detection of crime, apprehension of an offender or gathering of taxation.

External agencies or companies contracted to undertake processing of personal data on behalf of LPC must demonstrate, via a written agreement, that personal information belonging to LPC will be handled in compliance with the UK GDPR and DPA and that it has the necessary technical and organizational security measures in place to ensure this.

Any sharing of LPC data with external partners for the purpose of service provision must comply with all statutory requirements.

LPC will follow relevant guidance issued by the Government and the ICO for users of CCTV and similar surveillance equipment monitoring spaces to which the public, residents, service users and employees have access and will also strive to ensure that partner organisations involved in joint or multi-agency initiatives seek to do the same. LPC reserves the right to monitor telephone calls, emails and internet access in compliance with relevant legislation. This will be handled in line with guidance issued by the ICO.

The legal basis for this policy is the UK GDPR and DPA which provides the legal parameters for the processing of personal data. However, compliance with other legislation, Codes of Practice, policies and guidance also has relevance, such as:-

a. The Freedom of Information Act 2000
b. The Computer Misuse Act 1990
c. The Crime and Disorder Act 1998
d. Human Rights Act 1998
e. DUAA 2025

f. **Data Security**

LPC will process personal data in accordance with its Information Security Policy (and other related Policies and Procedures). To ensure the security of personal data, the Parish Council has appropriate physical, technical and organizational measures in place. All members and employees are required to comply with the Information Security Policy.

The UK GDPR and DPA requires that appropriate technical and organisational measures shall be taken to protect data against:

a. Unauthorised access;
b. Unauthorised or unlawful processing
c. Accidental loss, destruction, or damage

Appropriate technical and organizational security measures will include:

a. Using and developing technological solutions to ensure compliance with the data protection principles,
b. Using and developing physical measures to protect LPC assets,
c. Ensuring the reliability of any persons who have access to Lenham Parish Council information,
d. Reporting and investigating security breaches.

These obligations include the need to consider the nature of the data to be protected and the harm might arise from such unauthorised or unlawful processing or accidental loss, destruction, or damage.

All printout material, magnetic tape, diskettes, CD's or DVD's, manual files, hand written notes etc. which contact personal data and are no longer required, will be treated as confidential waste, and disposed of securely.

Where processing of Lenham parish Council data is to be carried out by a third party on behalf of LPC, the Clerk, they must ensure a third party provides sufficient guarantees in respect of the technical and organisation measures governing the processing to be undertaken.

Sharing Personal Data

LPC will not normally share personal data with anyone else, but may do so where:

a. There is an issue that puts the safety of our staff at risk,
b. LPC needs to liaise with other agencies – LPC will seek consent as necessary before doing this,
c. Our suppliers or contractors need data to enable to LPC to provide services to staff and residents, for example, IT companies. When doing this, LPC will:

    i. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law,
    ii. Establish a data sharing agreement with the suppliers or contractors, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any

personal data the Parish Council share,

iii. Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with LPC.

LPC will also share personal data with law enforcement and government bodies where LPC are legally required to do so, including for:

- The prevention or detection of crime and/or fraud,
- The apprehension or prosecution of offenders,
- The assessment or collection of tax owed to HMRC,
- In connection with legal proceedings,
- Where the disclosure is required to satisfy our safeguarding obligations,
- Research and statistical purposes, as long as personal data is sufficiently anonymized, or consent has been provided.

LPC may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our members of staff.

Where LPC transfer personal data to a country or territory outside the European Economic Area, LPC will do so in accordance with data protection law.

Data Retention and Disposal

LPC will not keep personal data for longer than is necessary for the purposes for which it was collected. All personal data will be held in accordance with the Parish Council's Data Retention Schedule, which is based on guidance issued by the National Association of Local Councils (NALC), the Local Government Association (LGA) and the Kent Association of Local Councils (KALC).

Once the retention period has expired, the data will be reviewed and securely deleted, shredded, or otherwise destroyed in a safe and confidential manner. In certain cases, data may be retained for longer periods if required by law, for archiving in the public interest, or for historical or research purposes, provided that appropriate safeguards are in place.

The Clerk is responsible for maintaining the Data Retention Schedule and ensuring that staff, councillors, and contractors are aware of and comply with retention requirements. This policy will be reviewed annually as per ICD guidance.

CCTV

The Parish Council uses CCTV in various locations around the Parish sites to ensure it remains safe. The Parish Council will adhere to the ICO's code of practice for the use of CCTV.

LPC do not need to ask individuals permission to use CCTV, but LPC make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Further information about the Parish Council's CCTV system can be found in our CCTV policy on the website.

Data Protection by design and default

LPC will use a Data Protection Impact Assessment (DPIA) toolkit to evaluate all new computer systems to help it determine how data protection compliance can be assured. In addition, all existing systems will be subject to periodic assessment.

DPIA toolkits provide a step-by-step approach to evaluate the proposed test, new or existing information systems to comply with the legislation. The DPIA process helps to identify weaknesses or risks to data losses or breaches and consider action that needs to be taken to ensure compliance where such compliance is not yet achieved. DPIA applies equally to paper as well as electronic data holdings systems.

The Clerk **must** be consulted when carrying out a data protection impact assessment.

Personal Data Breaches

LPC will make all reasonable endeavors to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, LPC will follow the procedure set out in our Security Incident and Data Breach Policy.

When appropriate, LPC will report the data breach to the ICO within 72 hours. Such breaches in a Parish Council context may include, but are not limited to:

a. The theft of LPC or personal electronic device containing non-encrypted personal data about members/ employees and/or residents,
b. Accidental disclosure of personal data to another person or organisation,
c. Inappropriate access to or use of personal data,
d. The theft of personal information, either paper based or electronic,
e. Accidental loss of personal data,
f. Information that has not arrived at its destination,
g. Fraudulent acquisition of personal data (Blaggers).

Training and awareness

Data Protection training and awareness is crucial so that all staff and councillors understand their responsibilities relating to data protection and the use of data protection. Failure to comply with the UK GDPR, DPA and the principles could lead to serious problems, and in some cases may result in significant fines or criminal prosecution.

It is LPC's policy that all staff and councillors complete the applicable training as required. This includes employees that do not have internet or email access. The Clerk will be responsible for ensuring that staff without internet or email access receive appropriate training.

Lenham Parish Council commitment to data protection

The Clerk will be accountable for ensuring compliance with this policy.

LPC will ensure that individuals handling personal information will be trained to an appropriate level in the use and control of personal data.

LPC have implemented a process to ensure all staff handling personal information know when are how to report any actual or suspected breach, and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner.

LPC will monitor and review its processing activities to ensure these are consistent with the principles of the UK GDPR and DPA and will ensure that its notification is kept up to date.

LPC will ensure that any new or altered processing identifies and assesses the impact on a data subject's privacy as a result of any processing of their personal data, and that appropriate Privacy Notices are maintained to inform data-subjects of how their data will be used.

LPC will review and supplement this policy to ensure it remains consistent with the Law and any compliance advice and Codes of Practice issued from time to time by the ICO.

Policy Review

The Clerk is accountable for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.