LAVERSTOCK AND FORD PARISH COUNCIL
GENERAL DATA PROTECTION POLICY

Purpose/Principles	To set out a Code of Practice on the lawful handling of data
Scope	Employees, Councillors, Volunteers, Contractors
Date adopted:	November 2026
Minute Reference:	PC25.139
Previous versions (Dates):	20 October 2025
Next review:	November 2027
Policy owner:	Full Council
Supersedes:	PC25.139

Contents

Policy

Appendix 1 – Data Audit Schedule

Introduction

Laverstock and Ford Parish Council is fully committed to compliance with the requirements of the Data Protection Act 2018 (“the Act”) and the UK General Data Protection Regulation (UK GDPR). The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the Council are fully aware of and abide by their duties and responsibilities under data protection legislation.

The Information Commissioner’s Office (ICO) is the UK’s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO has the power to impose enforcement action on organisations in the UK.

Statement of Policy

In order to operate efficiently, Laverstock and Ford Parish Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, service users, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within legislation to ensure this.

Laverstock and Ford Parish Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

To this end the council fully endorses and adheres to the Principles of Data Protection as set out in UK data protection legislation.

The Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with Six Principles of good practice. These Principles are legally enforceable.

The Principles require that personal information is:

1. used fairly, lawfully and transparently.
2. used for specified, explicit purposes.
3. used in a way that is adequate, relevant and limited to only what is necessary.
4. accurate and, where necessary, kept up to date.
5. kept for no longer than is necessary.
6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Policy Scope

This policy refers to data protection legislation, which provides conditions for the processing of any data defined as personal data and/or special category data.

Personal data is defined as data relating to a living individual (a data subject) who can be identified, directly or indirectly, from that data.

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 or condition
- Sexual life
- Biometrics (where used for identification)

There are separate safeguards for personal data relating to criminal convictions and offences – see Article 10 of the UK GDPR.

Data Protection Complaints

Individuals who are dissatisfied with how the Council has handled their personal data or exercised their information rights may submit a complaint to the Clerk (parish-clerk@laverstockford-pc.gov.uk)

The Council will investigate and respond to complaints within 14 days of receipt of the complaint.

If the complainant remains dissatisfied following the Council's response, they may complain directly to the Information Commissioner's Office (ICO – www.ico.org.uk). Tel: 0303 123 1113.

Lawful Bases for Processing Personal Data

Processing personal data is only legal if there is a lawful basis to do so. The lawful bases for processing are set out in Article 6 of the UK GDPR. The Council will ensure that at least one of these will apply whenever personal data is processed:

(a) Consent: the individual has given clear consent for their personal data to be processed for a specific purpose.
(b) Contract: the processing is necessary for a contract with the individual.
(c) Legal obligation: the processing is necessary for the Council to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for the Council to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for 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 cannot apply to public authorities processing data to perform official tasks.)

Conditions for Processing Special Category Data

Processing special category data is prohibited unless a lawful exemption applies. The conditions for processing are set out in Article 9 of the UK GDPR. The Council will ensure that at least one of these will apply whenever special category data is processed:

a. The individual has given clear consent for their personal data to be processed for a specific purpose.
b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
c. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
d. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
e. Processing relates to personal data which are manifestly made public by the data subject
f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g. Processing is necessary for reasons of substantial public interest
h. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
i. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices

Law Enforcement Purposes

The UK GDPR does not apply to sensitive processing for law enforcement purposes, which is covered by Part 3 of the Data Protection Act 2018 where sensitive processing is defined as:

a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;
c) the processing of data concerning health;
d) the processing of data concerning an individual's sex life or sexual orientation.

Law enforcement purposes are defined as 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.

Sensitive processing for law enforcement purposes is only permitted when:

- the data subject has given consent to the processing for the specific purpose or
- the processing is strictly necessary for a law enforcement purpose, the processing meets at least one condition in Schedule 8 of the Act

Laverstock and Ford Parish Council is not classed as a Competent Authority for Law Enforcement purposes and is not permitted to carry out sensitive processing as defined in Schedule 8 of the Act.

Handling of Personal/Special Category Data

Laverstock and Ford Parish Council will, through appropriate management and the use of strict criteria and controls:

- Fully observe conditions regarding the fair collection and use of personal information.
- Specify the purposes for which information is used.
- Collect and process information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of information used.
- Determine the length of time information is held.

- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.
- Ensure that the rights of data subjects can be fully exercised. These include:
    - The right to be informed
    - The right of access to one's personal information
    - The right to rectification
    - The right to erasure
    - The right to restrict processing
    - The right to data portability
    - The right to object
    - Rights in relation to automated decision making and profiling

If an individual makes a request relating to any of the rights listed above, the Council will consider each request in accordance with all applicable data protection laws and regulations.

No administration fee will be charged for complying with such a request unless the request is deemed to be unnecessary, excessive in nature, or a repeated request.

All subject access requests must be answered within 1 (one) month of the day after receipt. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The Council will notify the data subject of any such extension within one month of receipt of the request together with the reasons for the delay.

All requests received for access to, or deletion/rectification of personal data must be directed to parish-clerk@laverstockford-pc.gov.uk.

In addition, Laverstock and Ford Parish Council will ensure that:

- There is specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone handling personal information is appropriately trained to do so and is appropriately supervised.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance of handling data subject requests is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All managers and staff within the Council will take steps to ensure that personal data is kept secure at all times to prevent unauthorised, or unlawful, loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected by appropriate technical and organisational measures.

When engaging the services of contractors, consultants, partners or other agents, the Council will ensure:

- that they and their staff who have access to personal data held or processed for or on behalf of the Council, are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm.
- that any contracts/arrangements allow for data protection audits by the Council of data held on its behalf (if requested).

Councillors/Members of Parliament (MP)

The Council may share personal data with Councillors/MPs in the following circumstances:

- the Councillor/MP represents the ward in which the data subject lives.
- the Councillor/MP makes it clear that they are representing the data subject.
- the information requested is necessary to respond to a data subject's query/complaint.

Consent from the data subject is not required in these circumstances.

Data Protection Responsibilities

Under the Data Protection Act 2018, public authorities are required to appoint a Data Protection Officer. However, the provisions of section 7(3)(a) of the Act removes Parish Council's from this requirement. Laverstock and Ford Parish Council has not appointed a Data Protection Officer.

Data Controller: The Council is the Data Controller and has delegated overall responsibility for the day-to-day implementation of this policy to the Clerk. Email: parish-clerk@laverstockford-pc.gov.uk. The Clerk will receive appropriate training, as required.

Responsibilities of the delegated Data Controller

These delegated duties include the overall responsibility for monitoring internal compliance, informing and advising on data protection obligations, and acting as a contact point for data subjects.

The Clerk is responsible for ensuring:

- this Policy is implemented.
- the provision of data protection training for staff within the Council.
- for the development of best practice guidelines.
- for carrying out compliance checks to ensure adherence with data protection legislation throughout the authority.

Notification of Data Breaches

All staff are obliged to report any incidents involving information to ensure they are dealt with.

A data breach is a type of information security incident where the confidentiality, integrity or availability of personal data has been affected. The council will review incidents to assess if the risk to the rights and freedoms of the data subject(s) is likely to occur. In accordance with the UK GDPR, where the risk is likely, the council will report the data breach to the ICO **within 72 hours**.

Information Commissioner Registration

The ICO maintains a public register of data controllers and data protection officers. Laverstock and Ford Parish Council's registration number is Z7808610.

The Council will maintain payment of the ICO Data Protection Fee and ensure that its registration information remains accurate and up to date.

APPENDIX 1: DATA AUDIT SCHEDULE

What personal data do we hold? To whom does it relate? What data is it?	**Lawful basis for holding personal data** What is it for? Why do we have it?	**Sharing personal data** With whom do we share this data?	**Our internal processes** Who keeps this data? How long is it kept? Where is it held? How is it protected?
Staff			
Contract	HR, it is a contract	External professional advisers	Clerk, duration of employment plus 6 years, computer, password protected
PAYE	HR, legislative requirement	External professional advisers; HMRC; payroll company; nominated councillors for monthly finance checks	Clerk, Deputy Clerk & RFO, duration of employment plus 6 years, computer, password protected
Pension details	HR, legislative requirement	External professional advisers; payroll company; pension fund managers; HMRC; nominated councillors for monthly finance checks	Clerk, Deputy Clerk & RFO, duration of employment plus 6 years, computer, password protected
Bank details	HR, to pay staff salaries	Our bank; payroll company; nominated councillors	Clerk, Deputy Clerk & RFO, computer, password protected
Leave Form	HR, employment purposes	External professional advisers	Clerk, Deputy Clerk & RFO, computer, password protected
Staff appraisals and performance plans	HR, employment	Staffing committee members	Clerk, duration of employment plus 6 years, computer, password protected
Councillors		This is public knowledge	
Declarations of interest	Democracy, legislative requirement		Wiltshire Council and Clerk, term of office plus 4 years, computer & filing cabinet, password or lock & key
Personal contact details	Democracy, legislative requirement		L&FPC Officers, term of office plus 4 years, computer & filing cabinet, password or lock & key
Councillor email addresses	Democracy, legislative requirement		Ditto
Contractors and suppliers	Where we hold personal data about a natural person, not the data of a limited company or of another council.		
Contact details	Business, contact	External Professional Advisers	L&FPC Officers, see Document Retention Policy, computer or filing cabinet, password or lock & key
Invoices, purchase orders & quotations	Business, payment	Public inspection on audit	Ditto
Bank account details	Business, payment	Our bank	Ditto

What personal data do we hold? To whom does it relate? What data is it?	**Lawful basis for holding personal data** What is it for? Why do we have it?	**Sharing personal data** With whom do we share this data?	**Our internal processes** Who keeps this data? How long is it kept? Where is it held? How is it protected?
Insurance	Business, contract	External professional advisers	Ditto
References	Business, contact	External professional advisers	Ditto
Residents			
Electoral Register	Democracy	Public document required by law.	
Complaints, Freedom of Information requests and general correspondence from members of the public	Democracy	External professional advisers, MPs, principal councils.	L&FPC Officers strictly as necessary, 1 Year, computer or filing cabinet, none required
Community organisations			
Email addresses & phone numbers	Democracy, contact	Nobody without consent	L&FPC Officers, see Document Retention Policy, computer or filing cabinet, password or lock & key
Grant application forms	Democracy, service to community	External professional advisers	Ditto
Nominations of external committee members	Democracy, contact	Names become public knowledge; other data is confidential	Ditto
Planning			
Objections	Democracy, we are consulted on applications	Our objection or approval is a public document	L&FPC Officers, 1 year, computer or filing cabinet, none required.
Property			
Deeds	Property, council function	Public document registered at Land Registry	L&FPC Officers, indefinitely, computer or filing cabinet, password or lock & key
Licenses and Leases	Property, council function	External professional advisers	L&FPC Officers, indefinitely, computer or filing cabinet, password or lock & key
General Contacts			
Email addresses and phone numbers	Democracy, contact	Any reasonable request	L&FPC Officers, see Document Retention Policy, computer or filing cabinet, password or lock & key

- POLICY ENDS -