

## **1. BACKGROUND**

Laverstock and Ford Parish Council's Standing Orders requires under section 5(j) reviews of specific key policies and procedures at each annual meeting. This includes a review of the Council's policies, procedures and practices in respect of its obligations under freedom of information and data protection legislation.

## **2. SUMMARY**

The Council has adopted the following policies in order to meet its requirements under Interpretation Act 1978, Data Protection Act 2018, General Data Protection Regulation (EU regulation 2016/79), Freedom of Information Act 2000, the Local Government (Transparency Requirements) (England) Regulations 2015, Local Government Records Act 1962, Parochial Registers and Records Measure 1978, Local Government Act 1972, ss. 225-230, Local Audit and Accountability Act 2014, Accounts and Audit Regulations 2015 (SI 2015/234), Local Audit (Smaller Authorities) Regulations 2015 (SI 2015/184) and Smaller Authorities' Proper Practices Panel (SAPPP) 2025 edition.

General Data Protection Policy – adopted October 2025 (PC25.139). To be reconsidered November 2026. Contained in Annex One.

Document Retention and Deletion Policy – adopted December 2025 (PC25.151(b)). To be reconsidered October 2028. Contained in Annex Two.

IT Policy – adopted October 2025 (PC25.139). To be reconsidered November 2028. Contained in Annex Three.

Model Publication Scheme – adopted May 2025 (PC25.074). To be reconsidered December 2026. Contained in Annex Four.

Further, all current Councillors have read and signed their acceptance of responsibility for data protection with our General Data Protection Awareness Checklist. This checklist is included in the Acceptance of Office paperwork given to all new Councillors. All Officers and Councillors have been offered data protection training via LearningNest.

## **3. RECOMMENDATION**

That Council notes this review of the stated Policies in line with Standing Order 5(j) and resolves to continue with their relative reconsideration / readoption dates.

**ANNEX ONE** – adopted General Data Protection Policy

## **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:	20 October 2025
Minute Reference:	PC25.139
Previous versions (Dates):	21 May 2018
Next review:	November 2026
Policy owner:	Full Council
Supersedes:	Information Protection Policy, Data Protection Policy

### **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.

### **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

REPORT 26.056(e) FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

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](mailto: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.

REPORT 26.056(e) FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

### **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](mailto: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 Data Protection Act 2018 requires every data controller, who is processing personal data, to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

## APPENDIX 1: DATA AUDIT SCHEDULE

<b>What personal data do we hold?</b> To whom does it relate? What data is it?	<b>Lawful basis for holding personal data</b> What is it for? Why do we have it?	<b>Sharing personal data</b> With whom do we share this data?	<b>Our internal processes</b> Who keeps this data? How long is it kept? Where is it held? How is it protected?
<b>Staff</b>			
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
<b>Councillors</b>		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
<b>Contractors and suppliers</b>	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

REPORT 26.056(e) FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

<b>What personal data do we hold?</b> To whom does it relate? What data is it?	<b>Lawful basis for holding personal data</b> What is it for? Why do we have it?	<b>Sharing personal data</b> With whom do we share this data?	<b>Our internal processes</b> Who keeps this data? How long is it kept? Where is it held? How is it protected?
			& key
Invoices, purchase orders & quotations	Business, payment	Public inspection on audit	Ditto
Bank account details	Business, payment	Our bank	Ditto
Insurance	Business, contract	External professional advisers	Ditto
References	Business, contact	External professional advisers	Ditto
<b>Residents</b>			
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
<b>Community organisations</b>			
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
<b>Planning</b>			
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.
<b>Property</b>			
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
<b>General Contacts</b>			
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 -

## ANNEX TWO – Document Retention and Deletion Policy



# Laverstock & Ford Parish Council

## DOCUMENT RETENTION & DISPOSAL POLICY

Purpose/Principles	To provide guidance on effective record management to ensure the council meets its obligations under data protection regulations
Scope	Employees, Councillors, Volunteers
Date adopted:	15 <sup>th</sup> December 2025
Minute Reference:	PC25.151(b)
Previous versions (Dates):	None
Next review:	October 2028
Policy owner:	Finance and General Purposes Committee
Supersedes:	None

### 1. Introduction

- 1.1 The Council accumulates a vast amount of information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of documents.
- 1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.
- 1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.
- 1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the Council.

- 15 In contrast to the above the Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

## **2. Scope and Objectives of the Policy**

- 2.1 The aim of this document is to provide a working framework to determine which documents are:
- Retained – and for how long; or
  - Disposed of – and if so by what method.
- 2.2 There are some records that do not need to be kept at all or that are routinely destroyed in the course of business. This usually applies to information that is duplicated, unimportant or only of a short-term value. Unimportant records of information include:
- ‘With compliments’ slips.
  - Catalogues and trade journals.
  - Non-acceptance of invitations.
  - Trivial electronic mail messages that are not related to Council business.
  - Requests for information such as maps, plans or advertising material.
  - Out of date distribution lists.
- 2.3 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed.
- 2.4 Records should not be destroyed if the information can be used as evidence to prove that something has happened. If destroyed the disposal needs to be disposed of under the General Data Protection Regulations

## **3. Roles and Responsibilities for Document Retention and Disposal**

- 3.1 Councils are responsible for determining whether to retain or dispose of documents and should undertake a review of documentation at least on an annual basis to ensure that any unnecessary documentation being held is disposed of under the General Data Protection Regulations.
- 3.2 Councils should ensure that all employees are aware of the retention/disposal schedule.

## **4. Document Retention Protocol**

- 4.1 Councils should have in place an adequate system for documenting the activities of their service. This system should take into account the legislative and regulatory environments to which they work.
- 4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:

- Facilitate an audit or examination of the business by anyone so authorised.
- Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.
- Verify individual consent to record, manage and record disposal of their personal data.
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

4.3 To facilitate this the following principles should be adopted:

- Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations
- Documents that are no longer required for operational purposes but need retaining should be placed at the records office.

4.4 The retention schedules in Appendix A: List of Documents for Retention or Disposal provide guidance on the recommended minimum retention periods for specific classes of documents and records. These schedules have been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.

4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation have been removed.

## **5. Document Disposal Protocol**

5.1 Documents should only be disposed of if reviewed in accordance with the following:

- Is retention required to fulfil statutory or other regulatory requirements?
- Is retention required to meet the operational needs of the service?
- Is retention required to evidence events in the case of dispute?
- Is retention required because the document or record is of historic interest or intrinsic value?

5.2 When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the General Data Protection Regulations.

5.3 Documents can be disposed of by any of the following methods:

- Non-confidential records: place in wastepaper bin for disposal.
- Confidential records or records giving personal information: shred documents.
- Deletion of computer records.
- Transmission of records to an external body such as the County Records Office.

5.4 The following principles should be followed when disposing of records:

- All records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the Council being prosecuted under the General Data Protection Regulations.
- the Freedom of Information Act or cause reputational damage.

- Where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner.
  - Where documents are of historical interest it may be appropriate that they are transmitted to the County Records office.
  - Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).
- 55 Records should be maintained of appropriate disposals. These records should contain the following information:
- The name of the document destroyed.
  - The date the document was destroyed.
  - The method of disposal.

## **6. Data Protection Act 2018 – Obligation to Dispose of Certain Data**

- 6.1 The Data Protection Act 2018 ('Fifth Principle') requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. Section 1 of the Data Protection Act defines personal information as:
- Data that relates to a living individual who can be identified:
- a) from the data, or
  - b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.
- It includes any expression of opinion about the individual and any indication of the intentions of the Council or other person in respect of the individual.
- 6.2 The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely provided that the specific requirements are met.
- 6.3 Councils are responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations namely:
- Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
  - Personal data shall only be obtained for specific purposes and processed in a compatible manner.
  - Personal data shall be adequate, relevant, but not excessive.
  - Personal data shall be accurate and up to date.
  - Personal data shall not be kept for longer than is necessary.
  - Personal data shall be processed in accordance with the rights of the data subject.
  - Personal data shall be kept secure.
- 6.4 External storage providers or archivists that are holding Council documents must also comply with the above principles of the General Data Protection Regulations.

## **7. Scanning of Documents**

- 7.1 In general once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs.
- 7.2 As a general rule hard copies of scanned documents should be retained for three months after scanning.
- 7.3 Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs.

## **8. Review of Document Retention**

- 8.1 It is planned to review, update and where appropriate amend this document on a regular basis (at least every three years in accordance with the *Code of Practice on the Management of Records* issued by the Lord Chancellor).
- 8.2 This document has been compiled from various sources of recommended best practice and with reference to the following documents and publications:
  - *Local Council Administration*, Charles Arnold-Baker, 12th edition, Chapter 11
  - NALC LTN 40 – *Local Councils' Documents and Records*, January 2013
  - NALC LTN 37 – *Freedom of Information*, July 2009
  - *Lord Chancellor's Code of Practice on the Management of Records* issued under Section 46 of the *Freedom of Information Act 2000*

## **9. List of Documents**

- 9.1 The full list of the Council's documents and the procedures for retention or disposal can be found in Appendix A: List of Documents for Retention and Disposal. This is updated regularly in accordance with any changes to legal requirements.

**Appendix A: List of Documents for Retention and Disposal**

Document	Minimum Retention Period	Reason	Disposal
Minutes	Indefinite	Archive	Original signed paper copies of Council minutes of meetings must be kept indefinitely in safe storage. At regular intervals of not more than 5 years they must be archived and deposited with the Higher Authority
Agendas	5 years	Management	Bin (shred confidential waste)
Accident/incident reports	20 years	Potential claims	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Scales of fees and charges	6 years	Management	Bin
Receipt and payment accounts	Indefinite	Archive	N/A
Receipt books of all kinds	6 years	VAT	Bin
Bank statements including deposit/savings accounts	Last completed audit year	Audit	Confidential waste
Bank paying-in books	Last completed audit year	Audit	Confidential waste
Cheque book stubs	Last completed audit year	Audit	Confidential waste
Quotations and tenders	6 years	Limitation Act 1980 (as amended)	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Paid invoices	6 years	VAT	Confidential waste

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Document	Minimum Retention Period	Reason	Disposal
Paid cheques	6 years	Limitation Act 1980 (as amended)	Confidential waste
VAT records	6 years generally but 20 years for VAT on rents	VAT	Confidential waste
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)	Confidential waste
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)	Bin
Wages books/payroll	12 years	Superannuation	Confidential waste
Insurance policies	While valid (but see next two items below)	Management	Bin
Insurance company names and policy numbers	Indefinite	Management	N/A
Certificates for insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (SI 2753) Management	Bin
Town Park equipment inspection reports	21 years		
Investments	Indefinite	Audit, Management	N/A
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management	N/A
Members' allowances register	6 years	Tax, Limitation Act 1980 (as amended)	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Volunteer details	6 years		Confidential waste.
Document	Minimum Retention Period	Reason	Disposal
Information from other bodies e.g. circulars from	Retained for as long as it is useful and relevant		Bin

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

county associations, NALC, principal authorities			
Local/historical information	Indefinite – to be securely kept for benefit of the Parish	Councils may acquire records of local interest and accept gifts or records of general and local interest in order to promote the use for such records (defined as materials in written or other form setting out facts or events or otherwise recording information).	N/A
Magazines and journals	Council may wish to keep its own publications  For others retain for as long as they are useful and relevant.	The Legal Deposit Libraries Act 2003 (the 2003 Act) requires a local council which after 1 <sup>st</sup> February 2004 has published works in print (this includes a pamphlet, magazine or newspaper, a map, plan, chart or table) to deliver, at its own expense, a copy of them to the British Library Board (which manages and controls the British Library). Printed works as defined by the 2003 Act published by a local council therefore constitute materials which the British Library holds.	Bin if applicable

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Document	Minimum Retention Period	Reason	Disposal
<b>Record-keeping</b>			
<p>To ensure records are easily accessible it is necessary to comply with the following:</p> <ul style="list-style-type: none"> <li>• A list of files stored in cabinets will be kept</li> <li>• Electronic files will be saved using relevant file names</li> </ul>	<p>The electronic files will be backed up periodically on a portable hard drive and also in the cloud-based programme supplied by the Council's IT company.</p>	<p>Management</p>	<p>Documentation no longer required will be disposed of, ensuring any confidential documents are destroyed as confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.</p>
<p>General correspondence</p>	<p>Unless it relates to specific categories outlined in the policy, correspondence, both paper and electronic, should be kept. Records should be kept for as long as they are needed for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests.</p>	<p>Management</p>	<p>Bin (shred confidential waste) A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.</p>
<p>Correspondence relating to staff</p>	<p>If related to Audit, see relevant sections above. Should be kept securely and personal data in relation to staff should not be kept for longer than is necessary for the purpose it was held. Likely time limits for tribunal claims</p>	<p>After an employment relationship has ended, a council may need to retain and access staff records for former staff for the purpose of giving references, payment of tax, national insurance contributions and pensions, and in respect of any related legal claims made against the council.</p>	<p>Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.</p>

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

	between 3–6 months Recommend this period be for 3 years.		
--	---	--	--

Document	Minimum Retention Period	Reason	Disposal
<p><b>Documents from legal matters, negligence and other torts</b></p> <p>Most legal proceedings are governed by the Limitation Act 1980 (as amended). The 1980 Act provides that legal claims may not be commenced after a specified period. Where the limitation periods are longer than other periods specified the documentation should be kept for the longer period specified. Some types of legal proceedings may fall within two or more categories.</p> <p>If in doubt, keep for the longest of the three limitation periods.</p>			
Negligence	6 years		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Defamation	1 year		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Contract	6 years		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Leases	12 years		Confidential waste.
Sums recoverable by statute	6 years		Confidential waste.
Personal injury	3 years		Confidential waste.
To recover land	12 years		Confidential waste.
Rent	6 years		Confidential waste.
Breach of trust	None		Confidential waste.
Trust deeds	Indefinite		N/A

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Document	Minimum Retention Period	Reason	Disposal
<b>For Halls, Centres, Recreation Grounds</b>			
<ul style="list-style-type: none"> <li>• Application to hire</li> <li>• Invoices</li> <li>• Record of tickets issued</li> </ul>	6 years	VAT	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Lettings diaries	Electronic files linked to accounts	VAT	N/A
Terms and Conditions	6 years	Management	Bin
Event Monitoring Forms	6 years unless required for claims, insurance or legal purposes	Management	Bin. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Document	Minimum Retention Period	Reason	Disposal
<b>For Allotments</b>			
Register and plans	Indefinite	Audit, Management	N/A
Minutes	Indefinite	Audit, Management	N/A
Legal papers	Indefinite	Audit, Management	N/A

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Document	Minimum Retention Period	Reason	Disposal
<b>For Burial Grounds</b>			
<ul style="list-style-type: none"> <li>• Register of fees collected</li> <li>• Register of burials</li> <li>• Register of purchased graves</li> <li>• Register/plan of grave spaces</li> <li>• Register of memorials</li> <li>• Applications for interment</li> <li>• Applications for right to erect memorials</li> <li>• Disposal certificates</li> <li>• Copy certificates of grant of exclusive right of burial</li> </ul>	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI 204)	N/A

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Document	Minimum Retention Period	Reason	Disposal
<b>Planning Papers</b>			
Applications	1 year	Management	Bin
Appeals	1 year unless significant development	Management	Bin
Trees	1 year	Management	Bin
Local Development Plans	Retained as long as in force	Reference	Bin
Local Plans	Retained as long as in force	Reference	Bin
Town/Neighbourhood Plans	Indefinite – final adopted plans	Historical purposes	N/A

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Document	Minimum Retention Period	Reason	Disposal
<b>CCTV</b>			
Daily notes	Daily	Data protection	Confidential waste
Radio rotas	1 week	Management	Confidential waste
Work rotas	1 month	Management	Confidential waste
Observation sheets	3 years	Data protection	Confidential waste
Stats	3 years	Data protection	Confidential waste
Signing in sheets	3 years	Management	Confidential waste
Review requests	3 years	Data protection	Confidential waste
Discs – master and working	For as long as required	Data protection	Confidential waste
Internal Operations Procedure Manual	Destroy on renewal Review annually	Management	Confidential waste
Code of Practice	Destroy on renewal Review annually	Management	Confidential waste
Photographs/digital prints	31 days	Data protection	Confidential waste

In accordance with the Local Government Act 1972 s.227, archive services are provided by Wiltshire and Swindon History Centre [www.wshc.org.uk](http://www.wshc.org.uk)

**ANNEX THREE – IT Policy**

**LAVERSTOCK AND FORD PARISH COUNCIL IT POLICY**

Purpose/Principles	To provide guidance on the responsibilities for appropriate use of IT resources, both software and hardware, as well as other Council supplied resources.
Scope	Employees, Councillors, Volunteers, Contractors – collectively 'Users'.
Date adopted:	20 October 2025
Minute Reference:	PC25.139
Previous versions (Dates):	N/A
Next review:	November 2028
Policy owner:	Communications and Community Engagement Working Group
Supersedes:	Information Protection Policy, Removable Media Policy

**1. Introduction**

Laverstock and Ford Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by Council members, employees, volunteers, and contractors. Alongside the appropriate use of other information, usually delivered on paper media, created by or delivered via the Council.

**2. Scope**

This policy applies to all individuals who use Laverstock and Ford Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. Further, it applies to all Councillors and officers who access Council email (.gov.uk domain) or documents using a personal device.

**3. Acceptable use of IT resources and email**

Laverstock and Ford Parish Council IT resources and email accounts are to be used for official Council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

#### **4. Device and software usage**

Where possible, authorised devices, software, and applications will be provided by Laverstock and Ford Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

#### **5. Data management and security**

Staff and Councillors should not be allowed to access information until the Clerk is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

All sensitive and confidential Laverstock and Ford Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

All devices must:

- Be secured with a strong password/PIN/Biometrics and auto-lock after inactivity.
- Use encryption where available.
- Be kept updated with latest operating system and security patches.

Council data must be accessed only through approved applications (e.g. Outlook using LFPC account log-in).

Use of removable media (USBs, SD cards) for Council data is prohibited unless encrypted.

## **6. Disclosure of Information - Computer and Paper Based**

The disclosure of personal information to other than authorised personnel is forbidden. If there is suspicion of a User treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is to be reported to the delegated Data Controller (Clerk) who will take appropriate action.

Do not remove printed information from premises without the express consent of the information owner. Consent will only be given in exceptional circumstances

Protectively marked, personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

Disposal methods for waste computer-printed output and other media must be in accordance with Laverstock and Ford Parish Council's Document Retention and Disposal policy.

Distribution of information should be via the most secure method available.

Users should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

## **7. Network and internet usage**

Laverstock and Ford Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

## **8. Telephone communication**

Verify the identification of members before disclosing information. If in doubt, return their call using a known telephone number.

For external callers, verify their identity and their need to know the requested information. Telephone them back before releasing information and ask the caller to provide evidence of their identity.

- Ensure that you are authorised to disclose the information requested.
- Ensure that the person is entitled to be given this information.
- Ensure that the information you give is accurate and factual.

## **9. Email communication**

Email accounts provided by Laverstock and Ford Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

Personal or sensitive information is at risk if sent outside of the Council's network.

If an email is sent to an address that is not a Council domain address the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted.

Email should not be used for sending personal or sensitive information unless technical measures are in place to keep the message secure.

The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.

No identifiable personal information should be included when sending on emails.

The recipients of Laverstock and Ford Parish Council emails are prohibited from being forwarded, copied or blind copied to any third party within or outside of the Council.

Any Councillor email contact with a member of the public shall be directed to the Council Office for the attention of the delegated Data Controller (Clerk).

### **10. Password and account security**

Laverstock and Ford Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

### **11. Mobile devices and remote work**

Mobile devices should be secured with passcodes and/or biometric authentication.

When working remotely, users should follow the same security practices as if they were in the office. Further,

- Personal and council data must be kept separate (e.g. using distinct apps).
- Councillors must only use council data for council business.
- Council data must not be backed up to personal cloud accounts, public data and backup services (e.g. Dropbox, Google Drive) or shared with third-party apps.
- Users must not use publicly available wi-fi networks (e.g. in airports, hotels, cafes, restaurants and libraries) to access council data.
- Users must not circumvent Council controls, download and/or copy council data to or from their personal devices.
- Users must not screenshot, screengrab or take photos of Council data on their personal devices.

- Users must not allow their family members, friends or other individuals access to any device that is logged into the Council system and any data and systems accessed through it.
- Users must be aware of their surroundings when accessing Council data.
- Any personal device used may be subject to 'discovery in litigation'. This means that it could be used as evidence in a lawsuit against the Council. Your data could be examined by representatives of the Council and also by other parties in any lawsuit.
- Devices must allow for remote wipe or manual deletion of Council data.

## **12. Email monitoring**

Laverstock and Ford Parish Council reserves the right to monitor email communications to ensure compliance with this policy and applicable laws. Monitoring will be carried out in accordance with the Data Protection Act and GDPR.

## **13. Retention and archiving**

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

## **14. Reporting security incidents**

All suspected security breaches or incidents should be reported immediately to the Parish Clerk or, in their absence, the Deputy Clerk (or the Responsible Financial Officer if both Clerk and Deputy are absent), for investigation and resolution. Report any email-related security incidents or breaches to the Parish Clerk or, in their absence, the Deputy Clerk (or the Responsible Financial Officer if both Clerk and Deputy are absent), immediately.

## **15. Training and awareness**

Laverstock and Ford Parish Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All staff and Councillors will receive training on email security and best practices.

## **16. Compliance and consequences**

Breach of this IT Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

The Council may require confirmation that devices meet these security standards. No monitoring of personal use will be carried out beyond ensuring Council data is protected.

Councillors remain personally responsible for protecting Council data on their device.

On leaving office, Councillors must ensure all Council data is securely deleted and access revoked.

## **17. Policy review**

This policy will be reviewed every three years (or sooner should applicable legislation change) to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

## **18. Contacts**

For IT-related enquiries or assistance, users can contact [parish-clerk@laverstockford-pc.gov.uk](mailto:parish-clerk@laverstockford-pc.gov.uk).

All staff and Councillors are responsible for the safety and security of Laverstock and Ford Parish Council's IT and email systems. By adhering to this IT Policy,

REPORT 26.XXX FOI and Data Protection  
Author: Jon Sloan, Clerk  
Date: 29<sup>th</sup> April 2026

Laverstock and Ford Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

- POLICY ENDS -

REPORT 26.XXX FOI and Data Protection  
 Author: Jon Sloan, Clerk  
 Date: 29<sup>th</sup> April 2026

**ANNEX FOUR – Model Publication Scheme**

**Laverstock & Ford Parish Council**

**MODEL PUBLICATION SCHEME**

Information available from Laverstock & Ford Parish Council under the Model Publication Scheme.

<b>Purpose</b>	To set out a Code of Practice
<b>Scope</b>	Council employees, Councillors, and members of the public
<b>Date adopted</b>	12 <sup>th</sup> May 2025
<b>Minute Ref:</b>	PC25.074
<b>Previous</b>	n/a
<b>Next Review</b>	December 2026
<b>Policy Owner</b>	Finance & General Purposes Committee
<b>Supersedes</b>	None

<b>Information to be published</b>	<b>How the information can be obtained</b>
<b>Cost:</b> Charges per copy for hard copies see schedule at end	
<b>Class1 - Who we are and what we do</b> (Organisational information, structures, locations and contacts) This will be current information only. N.B. Councils should already be publishing as much information as possible about how they can be contacted.	(Hard copy or website)
Who's who on the Council and its Committees	Both
Contact details for Parish Clerk and Council members (named contacts where possible with telephone number and email address (if used))	Both
Location of main Council office and accessibility details	Both

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Staffing structure	Both
<b>Class 2 – What we spend and how we spend it</b> (Financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit) Current and previous financial year as a minimum	Both
Annual return form and report by auditor	Both
Finalised budget	Both
Precept	Both
Borrowing Approval Letter	Both
Standing Orders	Both
Financial Regulations	Both
Grants given and received	Both
List of current contracts awarded and value of contract	Both
Members' allowances and expenses	Both
Parish Plan (current)	Both
Annual Report to Parish Meeting (current and previous year as a minimum)	Both
<b>Class 4 – How we make decisions</b> (Decision making processes and records of decisions) Current and previous council year as a minimum	(Hard copy or website)
Timetable of meetings (Council and any committee/sub-committee meetings and parish meetings)	Both
Agendas of meetings (as above)	Both
Both Minutes of meetings (as above) – note this will exclude information that is properly regarded as private to the meeting.	Both
Reports presented to council meetings – note this will exclude information that is properly regarded as private to the meeting.	Included in agendas

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Responses to consultation papers	Hard copy where consultation was responded to on paper – online responses not available.
Responses to planning applications	Both
Bye-laws	Both
<b>Class 5 – Our policies and procedures</b>  (Current written protocols, policies and procedures for delivering our services and responsibilities)  Current information only	Both
Policies and procedures for the conduct of council business: Procedural standing orders Committee and sub-committee terms of reference Code of Conduct	Both
Policies and procedures for the provision of services and about the employment of staff: Internal instructions to staff and policies relating to the delivery of services Equality and Diversity policy Health and Safety policy Dignity at Work policy Safeguarding policy Policies and procedures for handling requests for information Complaints procedures (including those covering requests for information and operating the publication scheme)	Both
Records management policies (records retention, destruction and archive)	Both
Schedule of charges (for the publication of information)	Both

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

<p><b>Class 6 – Lists and Registers</b></p> <p>Currently maintained lists and registers only</p>	<p>(Hard copy or website; some information may only be available by inspection)</p>
<p>Any publicly available register or list (if any are held this should be publicised; in most circumstances existing access provisions will suffice)</p>	<p>Hard copy, if any</p>
<p>Assets Register</p>	<p>Website</p>
<p>Register of members' interests</p>	<p>Wiltshire Council website</p>
<p>Register of gifts and hospitality</p>	<p>Hard copy.</p>
<p><b>Class 7 – The services we offer</b></p> <p>(Information about the services we offer, including leaflets, guidance and newsletters produced for the public and businesses)</p> <p>Current information only</p>	<p>(Hard copy or website; some information may</p>
<p>Village Halls</p>	<p>Both</p>
<p>Parks, playing fields and recreational facilities etc</p>	<p>Both</p>
<p>Seating, litter bins, and memorials, etc</p>	<p>Hard copy</p>
<p>Bus Shelters</p>	<p>Hard copy</p>
<p>Services for which the Council is entitled to recover a fee, together with those fees (e.g. burial fees)</p>	<p>Hard copy</p>

Contact details:

REPORT 26.XXX FOI and Data Protection

Author: Jon Sloan, Clerk

Date: 29<sup>th</sup> April 2026

Tel: 07771 802839 Email: [parish-clerk@laverstockford-pc.gov.uk](mailto:parish-clerk@laverstockford-pc.gov.uk)

Web: [www.laverstockford-pc.gov.uk](http://www.laverstockford-pc.gov.uk)

**SCHEDULE OF CHARGES**

This describes how the charges have been arrived at and should be published as part of the guide.

<b>TYPE OF CHARGE</b>	<b>DESCRIPTION</b>	<b>BASIS OF CHARGE</b>
Disbursement cost	Photocopying @.25p per sheet (black & white)	Actual cost*
	Photocopying @.50p per sheet (colour)	Actual cost
	Postage	Actual cost of Royal Mail 2nd Class stamp

\*Actual cost incurred by the parish council.