Kidmore End Parish Council (KEPC)) / sign off May 2026 / Review May 2027

Data Retention Policy

Parish Clerk | Email: clerk@kepc.info

1. Introduction

1.1 Kidmore End Parish 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 ways. Records created and maintained by the Council are an important asset and 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.

1.2 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. It is imperative that documents are retained for an adequate period of time.

1.3 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.

1.4 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. Kidmore End Parish Council will endeavour to dispose of all electronic mail correspondence that is more than 2 years old, unless there is a statutory reason for keeping these documents [see point 5]. 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:

- 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.

2.4 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed. 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. 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 requirements. 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.
- 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.

4.2 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. This schedule has been prepared under the information from NALC legal topic note 40. 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 has 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.

6. 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.
- 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 or 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).

6.1 Records should be maintained of document disposals. These records should contain the following information:

- The name of the document destroyed.
- The date the document was destroyed.
- The method of disposal.

7. Data Protection Act 1998 AND GDPR 2018 – Obligation to Dispose of Certain Data.

The Data Protection Act 1998 ('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:

7.1 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. 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. Councils are responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations 2018 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.

7.2 External storage providers or archivists that are holding Council documents must also comply with the above principles of the General Data Protection Regulations.

8. Scanning of Documents

8.1 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. As a general rule hard copies of scanned documents should be retained for three months after scanning. 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.

9. Review of Document Retention

9.1 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). 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, 910h edition, Chapter 11

- Local Government Act 1972, sections 225 – 229, section 234

- SLCC Advice Note 316 Retaining Important Documents
- SLCC Clerks' Manual: Storing Books and Documents
- Lord Chancellor's Code of Practice on the Management of Records issued under

Section 46 of the Freedom of Information Act 2000

10. List of Documents

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.
- List of documents for Retention and Disposal
- Document Minimum retention Reason
- Minute books Indefinite Archive
- Scales of fees and charges 6 years Management
- Receipt and payment accounts Indefinite Archive
- Receipt books of all kinds 6 years VAT
- Bank statements (all accounts) Last completed audit year Audit
- Bank paying in books/cheque
- book stubs
- Last completed audit year Audit
- Quotations and tenders 6 years after end of contract Limitation Act 1980 (as
- amended)
- Paid invoices/cheques 6 years VAT/Limitation Act 1980 (as
- amended)
- VAT records 6 years VAT
- Petty cash, postage etc

Appendix B:

Overview

The GDPR, effective from 25 May 2018, is an EU regulation designed to protect personal data and privacy for all individuals within the EU, while harmonizing data protection laws across member states.

The GDPR (Regulation EU 2016/679) applies to any organization, public or private, that processes personal data of EU citizens, regardless of where the organization is based. It strengthens existing data protection rights and introduces new ones, giving individuals greater control over their personal information. The regulation also establishes independent supervisory authorities to monitor compliance and enforce the law.

Key Principles

GDPR is built on several core principles:

- Lawfulness, fairness, and transparency: Personal data must be processed lawfuly, fairly, and in a transparent manner.
- Purpose limitation: Data should be collected for specified, explicit, and legitimat e purposes.
- Data minimization: Only data necessary for the intended purpose should be colle cted.
- Accuracy: Personal data must be accurate and kept up to date.
- Storage limitation: Data should not be kept longer than necessary.
- **Integrity and confidentiality**: Data must be processed securely to prevent unaut horized access or breaches.

Rights of Individuals

- GDPR provides individuals (data subjects) with several rights:
- Right of access: Individuals can request access to their personal data.
- Right to rectification: Incorrect or incomplete data can be corrected.
- Right to erasure ("right to be forgotten"): Data can be deleted when no longer necessary or if consent is withdrawn.
- Right to data portability: Individuals can transfer their data between service providers.
- Right to be informed of breaches: Organizations must notify both authorities and affected individuals in case of serious data breaches.