

# NORTH DEVON COUNCIL – DOCUMENT RETENTION AND DISPOSAL POLICY

## Contents

Summary .....	1
1. Introduction .....	2
2. Scope & Purpose .....	2
3. Roles & Responsibilities .....	2
4. Retention Schedules .....	3
5. Retention & Disposal Protocol .....	3
5.1. Has the document been appraised? .....	3
5.2. Is retention required to fulfil statutory or other regulatory requirements?.....	3
5.3. Is retention required for evidence in the case of dispute(s)? .....	4
5.4. Is retention required to meet the operational needs of the service? .....	4
5.5. Is retention required because the document or record is of historic interest or intrinsic value? .....	4
5.6. Does all of the information contained within a document or record need to be retained? .....	4
6. Means of Disposal .....	5
7. Recording Disposals.....	5
8. Practical Arrangements for File Management and Disposal .....	6
9. Associated Documentation.....	6

## Summary

It is important that the council ensures effective management of its files, records and documents.

It is a legal requirement that the council keeps information, which permits identification of individuals, for no longer than is necessary for the purposes for which the personal information was collected.

The relevant Head of Service has overall responsibility for setting retention periods and for the destruction of documents/records in their service.

The Data Protection lead in each team/service shall ensure compliance with this policy insofar as ensuring personal data is not kept for longer than is necessary and that retention schedules are kept up to date.

Third parties must comply with the council's retention schedule when holding information on behalf of the council.

Retention schedules must be prepared and maintained recording how long documents and records may be retained and the justification for such retention period.

Documents/records must be destroyed appropriately and, where there is an identified business need, a record kept of the destruction.

## **1. Introduction**

North Devon Council (“the Council”) collects information from individuals and external organisations and generates a wide range of data and information which is recorded.

To facilitate the effective management of records in all formats (including paper and digital), Council officers must adopt a consistent and efficient approach for disposal and retention across the authority.

In managing our records and documents, officers must give regard to the Council’s duties and obligations, including:

- statutory or other regulatory requirements, including **Data Protection Legislation** (which includes all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended). It is a principle of Data Protection Legislation that personal data shall be: “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”
- maintenance of documentary evidence in case of disputes, complaints and/or challenges
- practical operational needs
- preservation of documents for historic or other value.

It is not possible to permanently retain all documents. There are issues with storage space as well as the possibility of breaching at least one principle of Data Protection Legislation. It is also of paramount importance to dispose of or retain documents in an orderly manner to reduce the burden of staff resources in the search of information in meeting the Council’s obligations under the Freedom of Information Act 2000 (FOI) or the Environmental Information Regulations 2004 (EIR).

## **2. Scope & Purpose**

The purpose of this policy is to provide a corporate policy framework to govern decisions on whether a particular document (or set of documents) should either be:

- retained, and if so in what format, and for what period
- disposed of, and if so when and by what method.

## **3. Roles & Responsibilities**

Heads of Service have overall responsibility for determining arrangements for managing documents within their service area and for decisions on disposal and retention of those documents.

Data Protection Lead for each team/service shall ensure, as far as possible, that their team/service is compliant with this policy, including making sure that their respective retention schedule is up to date and that data is being held and/or deleted in compliance with this.

The ICT Manager will be responsible for the erasure of data, or secure destruction of all redundant ICT equipment including hard drives, laptops, PCs, servers, USB devices or other digital media.

Heads of Service are responsible for returning all such redundant ICT equipment and digital media to the ICT service for secure erasure / destruction. This may include equipment and media whether or not it was originally supplied by the ICT service.

It is important all teams/services ensure that any third party that holds documents or records on the Council's behalf also comply with the principles of this retention policy.

Further guidance can be sought from the Data Protection Officer, the ICT team and the Information Management Group (IMaG).

#### **4. Retention Schedules**

Each team/service must create, retain and keep up to date a retention schedule to include, as a minimum, the class of record held, a description of the record, the retention period for the record, an explanation or authority for the retention period set and how the record is held. Each retention schedule is owned and must be maintained by the specified service/team (see Appendix 1). These are important documents which form part of the Council's Privacy Notice.

#### **5. Retention & Disposal Protocol**

The following section sets out the key issues to consider when making decisions about retention and disposal of records.

##### **5.1. Has the document been appraised?**

In most cases this should only take a few minutes or even less but it is a skilled task depending on the documents involved. It should therefore only be undertaken by officers who have sufficient operational knowledge to be able to identify the document and its requirements for continued need both within the service and corporate framework.

It is essential that before going further you make sure that no Freedom of Information or Environmental Information request has been received that may require this document/record.

##### **5.2. Is retention required to fulfil statutory or other regulatory requirements?**

The pieces of legislation which, either directly or indirectly, can impose minimum retention periods include:

- Tax Legislation; e.g. Value Added Tax Act 1994, Taxes Management Act 1970
- Statutory Registers; it is an implicit requirement that these records be maintained on a permanent basis, unless the legislation concerned stipulates otherwise
- Audit Commission Act 1998; auditors' access to documents in order to carry out their function
- Section 225 of Local Government Act 1972, concerns deposit of documents with

a proper officer of the Council

- Part VA of Local Government Act 1972, public access to certain documents relating to council and committee meetings
- Data Protection Legislation / Freedom of Information Act 2000, if there is an outstanding request or appeal the document needs to be retained until the appeal is over.

The above list should not be considered to be exhaustive.

### **5.3. Is retention required for evidence in the case of dispute(s)?**

Any document which may be required for legal proceedings should be kept until the threat of proceedings has passed. The Limitation Act 1980 specifies time limits for commencing litigation and therefore the starting point should be whether that period has now expired. The main time limits that are directly relevant to local government are:

- claims founded on simple contract or tort (other than personal injury claims) cannot be brought after the expiration of **6 years** from the date on which the cause of action occurred (e.g. debt recovery actions, and compensation claims in respect of sub-standard work, negligent advice, and damage to property)
- compensation claims for personal injury are barred on expiry of **3 years** from the date on which the cause of action occurred (this will usually be the date when the incident causing the injury occurred); **or** the date when the injured person first had knowledge of the injury
- claims that are based on provisions contained in documents that are 'under seal' are barred after the expiration of **12 years** from the date on which the cause of the action occurred.

### **5.4. Is retention required to meet the operational needs of the service?**

Documents or records might be useful for future reference purposes (e.g. training), as precedents, or for performance management (performance indicators, benchmarking and comparison exercises). A professional judgement needs to be made as to the usefulness of a particular document.

### **5.5. Is retention required because the document or record is of historic interest or intrinsic value?**

Some documents currently in storage may be of historic interest and/or even have some monetary value. Even if the document is of historical or monetary value, disposal, rather than retention by the Council, may be the more appropriate option but, for example, in the form of transfer to County Records; or even sale to an external body.

### **5.6. Does all of the information contained within a document or record need to be retained?**

When considering retention it may be necessary to consider applying more than one retention period. In this regard it may be that part of the record or document can be disposed of and it is only necessary to retain certain elements of a record or document which can then itself then be destroyed at a later date. It is essential to consider whether it is necessary to keep an entire record or document, in particular whether a document or record can be anonymised to remove personal data.

## 6. Means of Disposal

Records should be destroyed with the level of security required by the confidentiality of their contents.

For example, paper records containing sensitive personal data, or other restricted data should be disposed of in Confidential Waste. This will ensure that it is shredded and then the shredded paper handled securely, and disposed of securely, (i.e. a certificate of confidential destruction obtained). They should not be put in the normal recycling boxes or general waste bins.

With digital records, deletion of a file from a PC or records from a server is sufficient for internal disposal on the network by users. When ICT physically dispose of hardware, they will always ensure that all hard disks are shredded thus data cannot be recovered.

## 7. Recording Disposals

A Document Disposal Register must be maintained by each team/service (in line with the template at Appendix 2). A Freedom of Information request can refer to this list.

It is irrelevant and excessive to record every single destruction that the Council carries out. It is only necessary to record a disposal on the Document Disposal Register where there is a "business need" to record that a document once existed. Whether there is a business need to record a destruction is something for individual teams/services to determine depending on what they do, however it may be useful for statistical purposes or to have a record that certain action was taken by the Council.

The Document Disposal Register will be held on the corporate drive, in a single folder with a spreadsheet register for each service. It should record information relating to each disposal. It contains the following fields. Use the fields as relevant.

- Department
- Type of record
- File/record name
- Format
- Brief description of contents
- Date record created
- Date of record disposal
- Authorising/appraisal officer
- Method of disposal
- Disposal officer (for sensitive/confidential documents)

When disposing of records and recording disposal this could be done in a number of ways:

- It could be by group e.g. 'all complaint files closed in 2002'
- It can be by exception e.g. 'all complaint files closed in 2002, except case 1212 PPI St Brad's'
- It can be a unique file 'Customer Service project file on establishment of Ilfracombe One Stop Shop'.

NB. Please be sure that before disposing of any records that no request for an FOI disclosure has been received.

## **8. Practical Arrangements for File Management and Disposal**

Each service will have its own file management systems and often a unique set of issues relating to those files. In many cases services have their own methods for weeding out redundant files.

However, here are some practical suggestions which may help.

### Creating Files

- Index/reference files with a consistent approach within the team – make sure someone is responsible for the filing systems.
- When creating new records/files/folders consider in advance what the retention time will be and record it on the file to aid later disposal.
- Exemptions to stated disposal times should to be clearly flagged & recorded in the disposal register.
- Where document or case management systems are utilised, make sure that retention dates are built in to electronic systems.

### Managing Files

- Set appraisal objectives around effective file management and disposal. (Information Management is a core competency expected of managers).
- Check that relevant job descriptions and person specifications cover the essential skills of file and record management so that these are tested at recruitment.
- Timetable annual or more frequent agenda items onto team meetings to discuss file management

### Disposal of Files

Plan an annual 'clear-out day' to methodically go through files and dispose of files past their retention date. Update the disposal register.

## **9. Associated Documentation**

- Retention Schedules
- Disposal Register
- Information Security and Standards Policy
- Data Protection Policy
- Data Protection Guidance
- Procedure for Dealing with FOI and EIR Requests.