Borough Council of
King's Lynn &
West Norfolk

Records Retention And Disposal Policy

DRAFT

Contents

1. Introduction

1.1 In the course of carrying out its various functions and activities, the Borough Council of King's Lynn & West Norfolk (BCKLWN) collects information from individuals and external organisations and generates a wide range of data /information /documentation which is recorded in various formats.

1.2 The purpose of this policy is to ensure that the council manages a record through its life cycle from creation or receipt, through maintenance and use to final disposal (for destruction, transfer or permanent retention).

1.3 The policy also aims to ensure that all BCKLWN staff, elected members and service delivery partners are aware of what they must do to manage records in an effective and efficient way.

1.4 For the purpose of this policy no distinction will be made between data, records, documents and files, all of which hold information in or on them that in turn makes them part of the 'information life cycle'.

1.5 Modern day records management philosophy emphasises the importance of organisations having in place systems for the timely and secure disposal of records and information that are no longer required for business purposes. The General Data Protection Regulation significantly tightens up the rules on privacy and consent.

1.6 Premature destruction of documents could weaken our ability to defend litigious claims, lead to operational difficulties and result in failure to comply with the Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Data Protection Act 2018. In certain circumstances, the Information Commissioners Office has power to impose a financial penalty for breach of the 2016 General Data Protection Regulation (GDPR).

1.7 The council's policy and guidelines have evolved through two stages:

- Research into notable practice
- Additional input from staff.

1.8 By formalising the policy the council seeks to:

- Assist in identifying records that may be worth preserving permanently
- Prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration
- Provide consistency for the destruction of records not required permanently after specified periods
- Improved records management practices within the council.

1.9 The policy will be reviewed within 3 years from the date its approval.

2. Scope and purpose

2.1 The purpose of this policy is to provide a corporate policy framework to offer guidance and support to BCKLWN staff and members when making decisions on whether particular records and information should either be:

- Retained – and if so in what format, and for what period; or
- Disposed of – and if so when and by what method.

2.2 The guidelines are intended to cover all records and information from creation through to either destruction or retention.

2.3 Record retention policies were primarily created to define retention periods for paper records. However as more of the council business is performed electronically there is a need to define the retention periods of electronic records. These guidelines are relevant to records which are electronic, paper or records which have been transferred to another format such as microfiche.

2.4 Retention of documents may be necessary to:

- Meet operational needs
- Fulfil statutory or other regulatory requirements
- Evidence events/agreements in case of disputes
- Ensure the preservation of documents of historical or other value

2.5 There are however some records that do not need to be retained for any length of time. Standard Operating Procedure defines types of records that staff may routinely destroy in normal course of business. It usually applies to information that is duplicated, unimportant or only of short-term facilitative value. Such records or information include:

- Compliment slips
- Catalogues and trade journals
- Telephone message slips
- Non-acceptance to invitations
- Requests for stock information such as planning applications and regeneration plans
- Out of date distribution lists
- Working papers which lead to a final report
- Duplicated and superseded material including manuals and drafts

2.6 Permanent retention of records and information is undesirable, and appropriate disposal is to be encouraged for the following reasons:

- Indefinite retention of personal data may be unlawful
- There is a shortage of new storage space and what is available can be costly
- Disposal of existing paper records can free up office space for more productive activities
- Reduction of fire risk (for paper records)

- There is evidence that the de-cluttering of office accommodation can be psychologically beneficial for many workers.

2.7 Unstructured information systems

Email must not be used for storing council records. It is the responsibility of individuals to maintain their inboxes in compliance with data protection requirements and the council's retention and disposal policy and schedule. Emails that constitute a record which needs to be retained, including those containing person identifying information, must be stored in an appropriate filing system relevant to their confidentiality or business need.

Shared drives or other unstructured information storage solutions (including cloud based storage) used to store any council record should be managed in accordance with the Retention Schedule (Appendix A).

2.8 Structured systems storing person identifying information

All structured information management systems that store records containing person identifying information must be managed in accordance with the Retention Schedule. These systems must have a deletion or archival capability and where appropriate be able to identify a skeleton record (a subset of the original information) for continued retention.

2.9 The following council policies should also be considered when referring to the Records Retention and Disposal Policy:

- Data Protection Policy
- Data Quality Strategy
- FOI Publication Scheme
- ICT Asset Disposal Policy
- ICT Asset Management Policy
- ICT Computer Usage Policy
- ICT Email Policy
- ICT Internet Policy
- ICT Security Policy
- Information Risk Policy
- Records Retention and Disposal Policy
- Remote Working Personal Commitment Statement/Briefing Note
- Travelling Abroad with Council Devices Policy
- Use of Removable Media Policy

3. Records retention and disposal protocol

3.1 The Records Retention and Disposal Schedule (Appendix A) provides guidance on recommended and mandatory retention periods for specific classes of records and information.

3.2 If you wish to transfer permanent records to an archive please contact the Systems and Administration Manager, who will outline options for both paper and electronic records.

3.3 Where a retention period has expired in relation to a particular record or information a review should be carried out before a final decision is made to dispose. Such reviews need not necessarily be detailed or time consuming. Where the designated officer is familiar with the contents or where contents are straightforward and easily apparent then such an exercise may only take a few minutes.

3.4 In the event that a decision is taken to dispose of a particular record or set of records, then consideration should be given to the method of disposal.

3.4.1 Confidential Waste – making available for collection by a designated refuse service by placing paper documents containing personal data or confidential information in the blue 'confidential waste' bins. This applies to records listed as "Secure" in the Records Retention and Disposal Schedule.

3.4.2 Recycling – where practicable disposal should further recycling in line with the council's commitment to promoting an alternative waste disposal strategy. This applies to records listed as "Dispose" in the Records Retention and Disposal Schedule.

3.4.3 Deletion from a system - Documents held on an electronic document management system and main back office systems are subject to national discussions with various software suppliers to enable archiving of data and records. The Information Commissioner has advised that if steps are taken to make data virtually impossible to retrieve, then this will be regarded as equivalent deletion. ICT and the Systems and Administration Manager will advise on deletion.

3.4.4 Migration of documents to an external body – this method will be relevant where records or documents are of historic interest. The third party could be the National Archives (formally the Public Records Office). The council's Systems and Administration Manager will advise on this.

3.4.5 Electronic Devices and Removable Media - ICT will advise on this as specialised equipment or software may be required. Removable electronic media that have been used to store protectively marked data must be securely deleted before being re-used or disposed of, or securely destroyed where re-use is not possible or required. The normal delete function does not securely delete data as it can still be recovered using readily available recovery tools; ICT will perform the required secure sanitisation and disposal of ICT assets. All electronic equipment including computers, laptops and personal electronic devices, must be returned to ICT for re-use or disposal.

The disposal of data held on CDs, DVDs, USB Memory Sticks and any other removable media and devices should be the responsibility of the department who produced that data. It should be understood that any data belonging to BCKLWN that is discovered by a third party can cause controversy, adverse

publicity and other undesirable consequences for BCKLWN. If you have any doubts about the disposal of data in a safe and appropriate manner, then please contact the ICT Service Desk for further advice and information.

3.5 An audit trail of disposed records must be logged by keeping a record of the document or information disposed of, the date and method of disposal, and the officer who authorised disposal. The documenting of the disposal is particularly important due to the Freedom of Information Act. A log is maintained of records that are stored and disposed of by "Stor-a-File". Services should retain a local log of records that are disposed of using the form attached at Appendix B. Guidance on disposal is attached at Appendix C.

4. Roles and responsibilities

4.1 Members

Elected members are responsible for overseeing effective records management by the officers of the council and promoting adherence to this policy and the supporting framework.

Members also have access to records in the form of agendas, minutes, reports, briefing notes and correspondence with officers, community groups, members of the public, etc. These records can be sensitive particularly where the documents are exempt from publication, relate to individuals within their electoral ward, etc. Members therefore have a responsibility to manage and dispose of records in accordance with the Record Retention and Disposal Policy and Schedule.

4.2 Chief Executive

The Chief Executive has responsibility for the oversight and implementation of information risk management and fulfils the function of Senior Information Risk Owner (SIRO).

4.3 Management Team

Management Team are responsible for:

- approving and promoting this policy and the supporting framework;
- considering from time to time records management reports and ensuring due attention and
- resources are applied throughout the council to identified areas of need; and
- the operation and promotion of this policy and supporting framework within their service areas:
    - ensuring sufficient resources are allocated to meet corporate record management requirements;
    - ensuring those acting on behalf of the council receive appropriate training that is maintained and monitored on a regular basis, to ensure understanding and effectiveness;

- appropriate officers are appointed (and designated as required) to liaise and support records management groups and activities, and communicate records management to services; and
- records management is included in the business planning process.

4.4 Service managers

Responsibility for determining (in accordance with the Retention and Disposal Policy) whether to retain or dispose of specific documents rests with the individual service manager, in respect of those documents that properly fall within the remit or control of his/her service. The service manager will also need to audit legacy data to find out where it is and identify whether consent was granted correctly. They also need to delete records where it was not or where new consent cannot be obtained. The service manager will also need to ensure that privacy is designed into processes and services by default.

The rationale for this is that it is reasonable to both assume and expect that each service manager should be broadly conversant with the types of records received, generated and stored by his/her service.

Service managers may delegate the operational aspects of this function to one or more senior officers within their service. However in doing so they should ensure that any such officer is fully conversant with this Policy and is also familiar with the operational requirements of the service in relation to document retention/disposal and the General Data Protection Regulations.

4.5 Deputy Senior Information Risk Owner (SIRO)

The Deputy Senior Information Risk Owner (SIRO) is a senior officer who is familiar with information risks and supports the Chief Executive to provide the focus for the management of information risk across the council. They help establish and maintain assurance that information risk is being managed appropriately and effectively across the council and for any services contracted for.

4.6 Information Asset Owners (IAOs)

Each Head of Service is an Information Asset Owner (IAO) and is accountable to the SIRO for information assets within their business unit. Each IAO is responsible for how that information is held, used and shared. Each IAO will provide assurance that information risk is being managed effectively for those information assets that they have been assigned ownership. IAOs will be assisted in their roles by staff acting as Information Asset Administrators or equivalent that have day to day responsibility for management of information risks affecting one or more assets.

4.7 Information Asset Administrators (IAAs)

IAAs are operational staff with day to day responsibility for managing risks to their information asset and shall work with the IAO and with other supporting staff in risk management roles to manage information risk to their asset.

4.8 Individuals

Council employees, including contractors, consultants and volunteers employed to undertake council business, have a responsibility to document actions and decisions by creating and filing appropriate records and subsequently to maintain and dispose of those records in accordance with records management procedures.

4.9 Legal Services/Eastlaw

Can advise on whether minimum retention periods are prescribed by law, and whether retention is necessary to protect the council's position where the likelihood of a claim has been identified by the relevant service managers.

Legal Services/Eastlaw staff cannot be expected to possess the operational or background knowledge required to assess whether a particular document may be required by the service concerned for operational need. This is the responsibility of the relevant service manager or his/her designated officers.

4.10 Information Communications Technology (ICT)

The council's ICT Asset Policy states:

> The disposal of all ICT hardware assets is the sole responsibility of the ICT Department. Furthermore, no ICT hardware asset should be disposed of by any person, other than an authorised member of the ICT Department.
>
> The disposal of data held on CDs, DVDs, USB Memory Sticks and any other removable media and devices should be the responsibility of the department who produced that data. It should be understood that any data belonging to BCKLWN that is discovered by a third party can cause controversy, adverse publicity and other undesirable consequences for BCKLWN. If you have any doubts about the disposal of data in a safe and appropriate manner, then please contact the ICT Service Desk for further advice and information.

4.11 Systems and Administration Manager

The Systems and Administration Manager is available to provide Service Managers with advice and guidance on effective records management practices, and any queries regarding this Policy and the attached Retention and Disposal Schedule.

This Policy with be reviewed by the Systems and Administration Manager on a triennial basis unless any practical implications are identified sooner, at which time the guidance will be updated to reflect the latest position.

4.12 Commissioned services and suppliers

It is important to ensure contracts place clear obligations on suppliers to manage records, created or held by external agencies, on behalf of the council, in accordance with the Records Retention and Disposal Policy. A data sharing agreement should be considered to set out how a third party will be holding our data, the security arrangements they have in place and where data has been shared for a particular contract / project how data will be disposed of post-contract.

4.13 Partnership working

Where records are created as a result of partnership working there needs to be clearly defined responsibilities between BCKLWN and the partner organisation for the creation and management of records.

Where BCKLWN is the lead partner:

- the council's Records Retention and Disposal Policy will be applicable;
- the council will be responsible for the custody and ownership of the records;

Where another organisation is the lead partner:

- the records management policy and procedures of the lead organisation are
- applicable;
- the lead partner organisation will be responsible for custody and ownership of
- records;
- the council should identify and retain records relating to its role in the partnership required for its own business purposes. They should be retained in line with the council's records management policy.

Where there is no identified lead partner the council should ensure that provisions are made for one of the partners to assume responsibility for the management of the records.

A data sharing agreement should be considered to set out how a partner will be holding our data, the security arrangements they have in place and where data has been shared for a particular project how data will be disposed of post-project.

4.14 Home and mobile working

Modernised ICT systems, working practices and work styles have implications for records management particularly when working at home or from various locations. Please refer to the Remote Working Personal Commitment Statement/Briefing Note for further guidelines.

As a general rule, manual and electronic records containing personal data should not be removed from council premises. The ICT Computer Usage Policy states that:

> ..with the increased use of notebook computers and other mobile devices, the possibilities of confidential data accidently entering the public domain has risen dramatically. As such users of (but not exclusive to) a Laptop, Netbook, PDA, Tablet and Smart Phone's must also adhere to the following guidelines:
> - Do not allow anyone who is not an employee of BCKLWN to use the notebook. This especially applies to family and friends.
> - When using a notebook in the public domain, do not leave data on screen for longer than is necessary as this may be able to be viewed by people nearby.
> - If the notebook or mobile device contains confidential data, liaise with ICT to arrange for the notebook to have the data or device encrypted.
> - Do not leave a notebook unattended in a public place and do not store in a car overnight.
> - Do not use cloud data storage to synchronise any information between devices without prior ICT approval.

Additional guidance for home/mobile working is set out in the ICT Security Policy.

4.15 Data and media sent offsite

The ICT Security Policy sets out required practices. Should it be necessary to send media (CD's, DVD's USB memory sticks, etc.) off site that contain (or may possibly contain) sensitive or personal data, it must be sent by recorded delivery with a regulated and trusted courier.

All data should be classified according to the Government Security Classifications (GSC) scheme).

All records classified as 'Official - Sensitive' and above must be sent in an agreed encrypted format to minimise the risk of a data breach should the records go missing in transit. If in any doubt about sending data and media to suppliers, please contact the ICT Service Desk for further advice and guidance.

5. Legislative framework

5.1 Retention periods are often set by statute, whilst others are guidelines following notable practice in local government. The Retention and Disposal Policy reflects the requirements of the Data Protection Act 2018, General Data Protection Regulations, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

5.2 Data Protection Act 2018 (DPA)

The fifth data protection principle states that:
"..personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes."

If any personal detail is of sufficient interest to be archived, the DPA makes provisions for the personal data processed only for *'scientific, historical' or 'statistical' purposes'.*

This is conditional on meeting the criteria outlined in the Act.

5.3 Freedom Of Information Act 2000 (FOIA)

The FOIA gives anyone the right access to information held by the council.

There should be clearly defined policies and procedures for the retention and disposal of records. To ensure compliance the council has established a Retention and Disposal Schedule (Appendix A) which details record types held by all areas of the organisation.

5.4 Environmental Information Regulations 2004

The Environmental Information Regulations 2004 give people a right of access to information about the activities of public authorities that relate to or affect the environment, unless there is good reason for them not to have the information. This is sometimes referred to as a presumption in favour of disclosure.

5.5 Local Government Act 1972 (LGA) Part VA

This legislation governs public access to certain documents relating to council and committee meetings. Certain documents that form part of the public part of the agenda are required to be available for inspection by members of the public.

5.6 Tax legislation

Minimum retention for certain financial records are imposed by statutes such as the VAT Act 1994, and the Taxes Management Act 1970.

5.7 Statutory registers

Various local government statutes require registers to be kept of certain events, notifications, or transactions. It is implicit within such legislation that these records be maintained on a permanent basis, unless the legislation concerned stipulates otherwise.

5.8 The Audit Commission Act 1998

This provides auditors with a right of access to every document relating to the council that appears necessary for the purposes of carrying out the auditor's function under the Act.

5.9 General Data Protection Regulations (GDPR)

GDPR, if implemented correctly and in the right spirit, will help the council to foster the public's trust in the way it works. GDPR builds on current data protection legislation across European member states to consolidate this into a common set of standards that will apply to the processing of personal data for any European citizen, wherever that citizen may reside or wherever the processing takes place.

Under the GDPR, the council will need to have consent or one of five other specific legitimate reasons to hold and process individuals' data, including all legacy data. GDPR also stipulates the right of citizens:

- to be forgotten
- to make subject access requests at any time
- to have their data protected by processes of encryption or pseudonymisation[1]
- to prevent direct marketing
- to prevent automated decision-making and profiling, and
- to obtain and reuse any data held.

These obligations are applicable to both data controllers and processors. Data Controller means a person who determines the purpose for which and the manner in which any personal data are, or are to be, processed. The council is a Data Controller. Data Processor means any person or organisation that processes the data on behalf of the Data Controller.

Under Article 30 of GDPR, the council has responsibilities to document the personal data it processes as a controller and processor. These records will need to align with the Record Retention and Disposal Schedule.

The council will need to audit legacy data to find out where it is and identify whether consent was granted correctly. Records will need to be deleted where consent is absent or cannot be obtained. The council will also need to ensure that privacy is designed into processes and services by default.

In the absence of any legal requirements, personal data may only be retained as long as necessary for the purpose of processing. This means data is to be deleted e.g. when:

[1] Pseudonymisation" of data means replacing any identifying characteristics of data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified. It should be distinguished from anonymisation, as it only provides a limited protection for the identity of data subjects as it still allows identification using indirect means. Where a pseudonym is used, it may be possible to identify the data subject by analysing the underlying or related data.

.

- the data subject has withdrawn consent to processing;
- a contract has been performed or cannot be performed anymore; or
- the data is no longer up to date.

Exceptions may apply to the processing for historical, statistical or scientific purposes.

Expiration of the retention period

After the expiration of the applicable retention period personal data does not necessarily have to be completely erased. It is sufficient to anonymise the data. This may, for example, be achieved by means of:

- erasure of the unique identifiers which allow the allocation of a data set to a unique person;
- erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information);
- separation of personal data from non-identifying information (e.g. an order number from the customer's name and address); or
- aggregation of personal data in a way that no allocation to any individual is possible.

In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period, for example, because:

- the pool of data has grown so much that personal identification is not possible based on the information retained; or
- the identifying data has already been deleted.

Information obligations

In addition to other information obligations, in the context of data retention data subjects must be informed of:

- the retention period;
- if no fixed retention period can be provided – the criteria used to determine that period; and
- the new retention period if the purpose of processing has changed after personal data has been obtained.

6. Bibliography

ISO 15489 (BS ISO 15489-1:2001) Information and Documentation, Records Management, International Organization for Standardization
BS 10008:2014, Evidential Weight and Legal Admissibility of Electronic Information, The British Standards Institution
Information management, The National Archives (formally the Public Records Office).
Information and Records Management Society
Retention Guidelines for Local Authorities, The Records Management Society of Great Britain, 2003
Managing Records Retention and Disposal, Alison North, Ark Group, 2009
The Guide to the Environmental Information Regulations, Information Commissioners Office

The Guide to Freedom of Information, Information Commissioners Office
The Guide to Data Protection, Information Commissioners Office
The Guide to the General Data Protection Regulation (GDPR), Information Commissioners Office
Privacy Notice Code of Practice, Information Commissioners Office
ISO27001, Information security management systems, International Organization for Standardization
GDPR: Regulation (EU) 2016/679, European Parliament and of the European Council, 27 April 2016
Data Protection Bill 2017, Department for Digital, Culture, Media & Sport, 2017

7. Revision history

Policy name	Records Retention and Disposal Policy
Policy description	This policy sets out the Council's approach to the retention and disposal of records to ensure compliance with various acts of legislation and notable practice.
Document authors	Di Hill, Debbie Ess, Ged Greaves

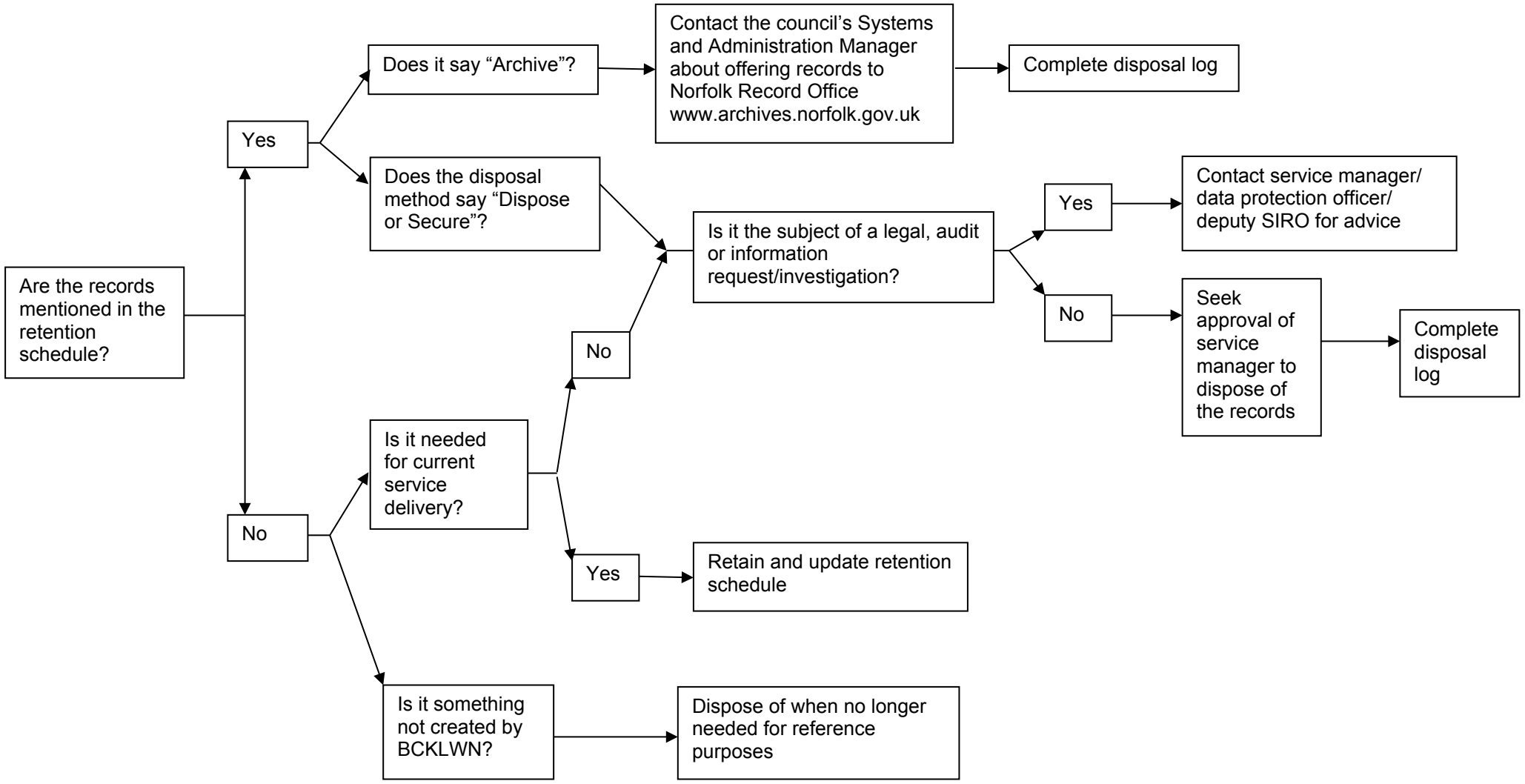
Version number	Date formally approved	Reason for update	Author	Review date
V0.1	30/09/2011	First draft	Diane Cross	
F1	26/01/2012	Final version	Karen Butler	2018
V0.1	14/02/2018	First draft	Ged Greaves	
V0.2	18/05/2018	Second draft	Ged Greaves	
V0.3	22/05/2018	Third draft	Ged Greaves	
V0.4	17/09/2018	Fourth draft	Ged Greaves	
V0.5	19/09/2018	Fifth draft	Ged Greaves	

Appendix A – Records Retention and Disposal Schedule

Appendix B – Disposal log

Date of disposal	Document/Information	Method of Disposal	Is there an outstanding FOI/SAR request on these records?	Notes	Amount (nbr of boxes, files, records)	Authorised	Directorate
28/06/2017	*Legal file relating to the purchase of land at Main Street.*	*Shred Station – Shredded*	*No*	*Land disposed of in 1991.*	*1 file, approx. 200 pages*	*Name Job Title*	
28/06/2017	*Project files relating to service reviews conducted in 2010.*	*Shred Station – Shredded* *Data files deleted*	*No*		*2 files approx. 400 pages*	*Name Job Title*	

Appendix C – Outline disposal flowchart



Appendix D - Disposal checklist

1. Has the document been appraised?

Before a record is designated for disposal the nature and contents of the record needs to be ascertained. This process may only take a few minutes. However, this can be a skilled task depending on the complexity of the record concerned. This evaluation process should only be undertaken by officers who possess sufficient operational knowledge to enable them to identify the record concerned and its function within both the individual service and corporate framework.

2. Is retention required to fulfil statutory or other regulatory requirements?

Identifying how long records need to be kept is one of the most important areas to be addressed. The Retention Schedule at Appendix A is the key tool for facilitating how long records need to be kept. As a rule of thumb it should be possible to dispose of most records and ordinary correspondence type records after seven years. This is calculated by allowing a statutory limitation period of 6 years plus a further year as an added safeguard.

However, there are exceptions to this that include legal records and notices, records which the Council is legally required to maintain in a public register, correspondence about ongoing contracts and building works less than 15 years old, leases and matters about which a dispute is known or anticipated. However, some records will be of temporary nature and can be disposed of much more quickly.

If there is any doubt regarding the correct retention period for a certain record reference may need to be made to legislation that stipulates minimum retention periods for particular records in local government. In addition advice can be sought from the Legal Section of the Council. However, there may come a point at which the balance of convenience and safety rests with retaining a record rather than conducting extensive inquiries to determine whether it is safe to dispose of the record.

3. Is the retention required for evidence?

Occasionally, the Council becomes involved in disputes with third parties. Such disputes can result in the party who is dissatisfied bringing legal proceedings against the Council. Alternatively, the Council may wish or be required to institute legal proceedings against an individual or organisation. Such proceedings may be civil or criminal in nature. Where a dispute arises, or litigation has been commenced it is important that the Council has access to all records that are relevant to the matter. Without such records there is the danger that the Council's position will be compromised.

Specific time limits are laid down for the commencement of litigation. The time limits are different according to the nature of the claim. The starting point therefore, is that the retention period is the length of time that has to elapse before a claim is barred. The Legal Service at the Council will be able to give advice if there are areas of doubt.

4. Is retention required to meet the operations needs of the service?

In some cases retention may be desirable even though no minimum retention period applies, or has expired. Records may be useful for future reference purposes, as

precedents, or for performance management. Skilled judgment may be needed to assess the usefulness of a particular document.

5. Is the document or record of historic interest?

In most cases this consideration will not be applicable. However, some records currently in Council storage may be of historic interest. If the record is of historic interest consideration may be given to transfer to the County Archivist rather than retention or disposal by the Council.