Records Management and Retention Policy

April 2018

districtnk
100 flourishing communities
North Kesteven District Council

Alternative Formats

This document can be made available in large print, Braille, audio tape, electronic formats such as CD, or in a different language. Our website is ReadSpeaker enabled. For a copy please contact the Corporate Information Team at the Council using the following options:

Phone: 01529 414155 (main switchboard)

Fax: 01529 413956

Web: www.n-kesteven.gov.uk

Email: equality@n-kesteven.gov.uk

Corporate Information Manager
North Kesteven District Council
Kesteven Street
Sleaford
Lincolnshire
NG34 7EF

Introduction
Information is one of the Council's corporate assets; in the course of carrying out its' various functions, the Council accumulates information from both individuals and external organisations. The Council also generates a wide range of data, which is recorded in documents and records. These documents and records are in several different formats, examples of which include (but are not limited to) communications such as letters, emails and attendance notes; financial information including invoices, statements and reports; legal documents such as contracts and deeds; and information relating to various types of applications, including forms, plans, drawings, photographs and tape recordings. For the purposes of the Policy, the terms 'document' and 'records' include information in both hard copy, electronic and audio-visual formats.

The General Data Protection Regulations (GDPR) has a focus on effective records management. Issues relating to management of records are important to the ongoing business and legislative obligations of the Council. Specifically, the Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act 2000 and the General Data Protection Regulations requires evidence that comprehensive records management arrangements are in place. The key purpose of records management is to:

- Create and capture authentic and reliable records which provide evidence of the Council's activities and decisions and which demonstrate its accountability;
- Secure, maintain and preserve those records for as long as they are required and to provide access to them as necessary to support the Council's operations and fulfil its obligations under access to information legislation;
- Identify those records which will form a significant part of the historical record of the Council's activities and make provision for their permanent or long term preservation;
- Identify those records that are vital to the continuance of the Council's business and protect these against disaster;
- Destroy records that are no longer required, having regard to statutory record-keeping requirements, thereby promoting the efficient use of physical and electronic storage space.

As part of being an open and transparent organisation, having a robust policy ensures that members of the public understand what information the Council holds and for how long it is kept. This also ensures the Council is not spending money unnecessarily storing information; equally it will be easier to search for and find information reducing the amount of resource wasted in locating it. It may be necessary to retain specific documents in order to fulfil statutory or regulatory requirements and also to meet operational needs. Document retention may also be useful to evidence events or agreements in the case of disputes, and also to preserve information which has historic value. Premature destruction of documents could result in inability to defend litigious claims, operational difficulties and failure to comply with access to information legislation.

Equally, the retention of all documents and records is impractical and appropriate disposal is important. Disposal will assist the Council to maintain sufficient electronic and office storage space and will de-clutter office accommodation, resulting in a more desirable working environment. In addition, lengthy or indefinite retention of personal information could result in the Council breaching the General Data Protection Regulations. This is why it is important that the Council has a system in place for the timely and secure disposal of documents and records that are no longer required for business purposes. In addition, the Policy should help to ensure that the Council archives records and documents that are of historical value appropriately for the benefit of future generations.

Records Management
Records Management is a corporate requirement; hence this Policy applies to all groups, services, and employees of the Council. It also links to other key Council documents and policies, in particular Freedom of Information and Environmental Information, Data Protection, Information Security, Internet and E-mail procedures. Records Management is part of a suite of policies and

procedures which are necessary to ensure that full and accurate records of all activities and decisions of the Council are created, managed and retained or disposed of appropriately.

North Kesteven District Council will ensure that reliable and usable records are created, maintained and made accessible for as long as they are required to support the business of the Council. We will ensure this by:

- Having timely access to all relevant information and that records are kept in line with legal, administrative and financial requirements;
- Records are managed effectively and efficiently to appropriate standards;
- Records are maintained in a secure environment with good conditions for their physical preservation and storage and which allows access as needed;
- Records are kept in accordance with the schedules drawn up for their retention, having regard to legal requirements and recognised good practice, and are safely disposed of after the expiry of their retention period in accordance with legal and regulatory obligations;
- The Council complies with all legislation and regulations concerning the proper management of records. This includes Freedom of Information Act 2000, General Data Protection Regulations, Public Records Acts 1958 and 1967, Environmental Information Regulations 2004, and so on;
- Records are accessible to Officers to support them in making informed and proper judgments in the course of their work;
- Records are accessible to the public in accordance with the Council's Publication Scheme;
- Records are kept securely and protected from accidental or deliberate loss or destruction;
- All employees are aware of their obligations in respect of the filing, retention and disposal of records.

This Policy covers the time from when a document or record is created within the Council to the time it is either destroyed or preserved permanently within the archives. The stages of records are:

- Create or receive information in the form of records;
- Classify records into a logical system;
- Maintain and use the records;
- Destroy or archive records in line with retention guidelines.

There are five key objectives:

Maintain and manage records effectively throughout their lifecycle
The Council has to manage and maintain records from when they are created to when they are destroyed or archived. The process has to account for all the Council's actions and decisions. For example, drafts of documents may be requested under Freedom of Information. As such, the Council needs to be aware of the lifecycle of the documents and records it creates so that it can provide transparency of its decisions. At the same time, the lifecycle approach ensures that records are managed and maintained for as long as they are required. In doing so, it provides an audit trail for decisions.

Clear Retention and Disposal Arrangements
The Council needs to know what it has to keep and for how long. In some cases records such as asbestos have retention periods of over 40 years. The retention guidelines that will be agreed within Divisions will address their business needs as well as their service specific statutory requirements. In some cases, the Council has to retain records permanently and these will be transferred to the archives.

Accessible Filing
When records are filed, they have to be retrievable. To retrieve records, a common approach to filing would be preferred with common naming conventions so that files can be tracked and found.

The naming convention for files is needed to establish the context of the record and identify who created the document.

Ensure Security of Data
The Council needs to ensure that data is stored in a secure environment with appropriate security and backup systems in place. Access and the use of data should be appropriate to the data user and comply with relevant legislation.

High Quality Information
The Council recognises that there are a number of key characteristics of good quality data. The data on which we report and make decisions on should be:
• Accurate – Data should be sufficiently correct for its intended purposes;
• Valid – Data should be recorded in an agreed format and used in compliance with recognised Council and national standards;
• Reliable – Data should reflect stable and consistent data collection processes across the Council;
• Timely – Data should be available within a reasonable time period, quickly and frequently enough to support information needs;
• Relevant – Data captured should be relevant to the purpose for which it is used;
• Complete – Data should be captured based on the information needs of the Council;
• Secure – Data should be stored securely and confidentially;
• Accessible – Data should be easily available by those who need it.

General Data Protection Regulations (GDPR)
The GDPR has five key areas of focus in relation to records management, which is explored further in the Council's Data Protection Policy:
• Control – The Council should enable data subjects to control the processing of their personal data;
• Minimise – The Council should restrict the amount of personal data it processes to a required minimum;
• Inform – The Council should let data subjects know when their personal information is at risk;
• Demonstrate – The Council, as a data controller and processor, must be able to show compliance;
• Enforce – The Council's privacy notice must be understood and used correctly by all Divisions.

Retention and Disposal of Documents and Information
Information will be assessed and a retention period set according to the following principles:

- Statutory requirements: information will be retained for only as long as is required by statute;
- Ongoing business need: information will be retained for only as long as it is required to run the organisation effectively. Storing information costs money, therefore storing information for longer than is necessary incurs unnecessary costs;
- Best practice: information will be retained if best practice indicates this would be of benefit; best practice can be drawn from respected external sources.

Management of Information – Databases
Information held in databases can be constantly evolving, however this does not mean that it is exempt from the Policy. The Council will ensure that the information held in databases it manages, owns or uses is accurate and up to date and not retained beyond the time limit set out in the retention schedule and/or information asset register. Where there seems to be no justified reason to hold personal or sensitive information it must be destroyed immediately, unless the information owner can present a sound business reason or statutory requirement.

In managing information held in databases the Council will correct errors on discovery and dispose of out of date records in line with the retention schedule. Information collected in error or found to be a duplicate will be deleted. Where information needs to be retained for statistical or research purposes the information owner must ensure that all such information is anonymised and meets our statutory obligations for the management of personal or sensitive information.

Management of Information – Email

Emails and attachments relating to Council business are corporate records and must be managed in accordance with the Council's retention schedule. Email users need to manage their accounts effectively and proactively and retained emails should be filed appropriately.

Roles and Responsibilities
All employees who create, process or use information on behalf of the Council are information users and are responsible for ensuring that information is stored and handled appropriately.

Heads of Service and Managers
Heads of Service and Managers are responsible for determining (in accordance with the retention schedule) whether to retain or dispose of specific documents within the remit of their service area. However, Heads of Service and Managers may delegate the operational aspect of this function to one or more Officers within their service area. Heads of Service and Managers are ultimately responsible for ensuring that information is retained for the correct period and then disposed of or transferred appropriately and that the retention schedule is accurate and up to date. In addition, when information is of historic value the relevant Head of Service and Manager is responsible for deciding if information earmarked for disposal should be disposed of or offered to the archive service.

The retention schedule sets out how long information should be kept before it is disposed of or transferred to the archive service, however Heads of Service and Managers should seek guidance from the Corporate Information Team if they feel that changes or modifications to the schedule are required.

Heads of Service and Managers should also ensure that all records within their Division have an identified owner, responsible for their management whilst in use. They should also ensure that a satisfactory audit trail exists for records destroyed according to the retention schedules and ensure that business recovery plans are in place to allow continuity of service in event of a disaster.

In addition, Heads of Service and Managers should ensure their Division/Teams, including contractors, consultants and volunteers employed to undertake Council business, follow procedures for the management and storage of electronic and hard copy records. They are also responsible for ensuring that their Division/Teams comply with the Policy and follow associated guidance relating to specific responsibilities.

Senior Information Risk Owner (SIRO) and Information Asset Owners (IAOs)
The SIRO has overall responsibility for managing records and associated risks, whilst the Information Asset Owners have the responsibility to ensure information is held and used appropriately, retained for the correct period of time and then correctly disposed of or transferred to the archives. In essence, the SIRO is supported by a team of specialists (IAOs), with day to day responsibility for records management. The IAOs are also responsible for ensuring their Teams comply with the retention schedule and ensuring it is reviewed and updated on a regular basis. They also have a role in supplying local expertise relating to retention periods and updating the relevant parts of the retention schedule in consultation with the Corporate Information Team.

Data Protection Officer
The Data Protection Officer (DPO) will provide advice and assistance to employees regarding retention, disposal and transfer of information. In addition, the DPO will ensure that management of the Council's records complies with legal and professional obligations; advise Officers on records management; implements the Policy; and helps to maintain the retention schedule.

All Employees
Information created must be managed to ensure that it is correctly located and retained for the appropriate period in accordance with the retention schedule. All employees have a responsibility to ensure that they dispose of information and data in an appropriate way, taking into consideration the format and sensitivity of the information or data.

Employees have a duty to report loss of information, including technical problems, theft and human error to their line Manager and Data Protection Officer who will take appropriate action (please see Data Protection Policy). Employees have a duty to report problems or anomalies with the retention schedule and the Policy to the Data Protection Officer as soon as a problem is noticed. They also have a role in supplying local expertise relating to retention periods. They must also highlight any potential delays in disposal to the Data Protection Officer.

In addition, all employees should file records appropriately and ensure that all records, regardless of format, are stored safely in suitable conditions.

Disposal
It is essential to take into consideration the format and the sensitivity of the information when deciding on the appropriate disposal method. Paper information that is sensitive, or has potential legal repercussions or a high risk of reputational damage to the Council should be placed in the confidential waste bins to ensure the information is disposed of securely. Examples of this include information regarding personal data or potentially commercially sensitive information. Confidential waste bins are available and are located around the Council's offices in order that confidential documents can be destroyed. It is essential that any documents which are to be thrown away and contain confidential, sensitive or personal data must be disposed of in this way in order to avoid breaches of confidence or breach the General Data Protection Regulations.

Disposal of documents other than those containing confidential or personal data may be disposed of by binning, recycling, deletion (in the case of electronic documents), and the transfer of documents to external bodies. Transfer of documents to external bodies will be unusual but could be relevant where documents are of historic interest and may be sent to the archives.

Records of disposal should be maintained by each service area, and should detail the document disposed of, the date and the Officer who authorised the document's disposal. Information that has reached the end of its retention period and is not required should be disposed of or transferred to the archive service without delay.

Electronic information must be treated in the same way as physical information; therefore electronic information must be disposed of once it has reached its set disposal date. If any delay is anticipated then this should be raised to the Data Protection Officer with a timescale of when the information will be disposed of. Managers must ensure that a brief description of the destroyed information is kept.

Information Wrongly Disposed Of
Wrongful disposal may occur as a result of technical problems, human error or by deliberate act. Wrongful disposal of information must always be reported on discovery to the relevant Manager and Data Protection Officer to allow them to identify any gaps in the information and review what action needs to be taken.

The Data Protection Officer will review the circumstances surrounding the wrongful disposal and, where appropriate, procedures will be changed in order to ensure further disposals in error cannot take place or that such a risk is mitigated.

Information Wrongly Kept

Under the Data Protection Act 1998 it is illegal to retain information for longer than is necessary. Wrongful disposal may occur as a result of technical problems, human error or by deliberate act. Wrongful disposal of information must always be reported on discovery to the information owner and Corporate Information Team. The information must be disposed of immediately and a log of the decision and circumstances surrounding the incident must be added to the schedule.

The Data Protection Officer will review the circumstances surrounding the information wrongly kept and, where appropriate, procedures will be changed in order to ensure further disposals in error cannot take place or that such a risk is mitigated.

Policy Review

This Policy will be formally reviewed every two years to ensure it continues to be relevant and current. In some circumstances it may be necessary to review this Policy more frequently in response to specific events.