Document and Management Policy

Author: Robert Beane (Veritau Ltd)
Date: February 2016
Approval: Management board
Audience: Council officers and members

Policy statement

Recorded information, in the form of records or other documents, is an important corporate asset and effective management of these records and documents is necessary to support the council’s core business functions and statutory obligations.

Purpose and objectives

The aim of this policy is to provide a framework for managing the council’s records and documents. Effective management of records and documents helps the council to achieve the following policy objectives:

- Deliver quality services by having timely access to meaningful and appropriate information;
- Make informed decisions;
- Be open and transparent;
- Respond appropriately to information requests from the public; and
- Protect records from threats, including unauthorised or accidental disclosure.

Scope

This policy applies to employees, contractors, volunteers and other unpaid or temporary workers (for example, work experience placements). It does not apply to NYCC schools although schools may wish to apply the same principles as set out in this policy.

The policy includes all physical and electronic information, documents and records processed by the council throughout their lifecycle, regardless of the technology needed to create them. The policy also covers all systems, procedures and devices that create, maintain and disseminate information, documents and records.

The council is implementing a document management solution, covering all print, scanning and internal and external postal services. This policy governs the use of all devices which are
used for the creation of physical records and documents, such as printers, scanners and multi-functional devices (MFDs).

Information, documents or records which have been shared or loaned by other local authorities, businesses and organisations should be treated in the same manner as records created by the council and subject to the same requirements for maintenance, security and use referred to in this policy. Reasonable care must be taken to ensure records can be tracked, located and returned to source as required.

Roles and responsibilities

This section is to be read in conjunction with the information governance policy.

- **Everyone** who has responsibilities for creating, receiving, maintaining, using and disposing of documents and records must follow the council’s authorised procedures. All employees who handle documents and records must complete mandatory training with reference to information management and must familiarise themselves with this policy.

- **Managers** must familiarise themselves with and ensure that their staff are aware of this policy and identify, where appropriate, training for staff in relevant records and document management procedures as required.

- The **senior information risk owner (SIRO)** takes ownership and responsibility of the risks associated with keeping the council’s information secure and sharing it responsibly. The SIRO chairs meetings of the corporate information governance group (CIGG) which decides on the council’s strategy for governing its information resources.

- An **information asset owner (IAO)** is an appointed individual who is responsible for ensuring that specific information assets within their service are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the council is fully exploited. They should also identify and record information risks and help develop appropriate mitigation strategies.

- **Corporate directors and assistant directors** must ensure that information is treated as a valuable resource and that document and records management procedures are embedded into normal business processes. They must ensure that appropriate employees are designated to champion records and document management for
their directorate. Each corporate director is also responsible for establishing and maintaining an information asset register to record their information assets.

- **Directorate information governance champions (DIGCs)** monitor and co-ordinate information governance activities within their directorate. They will ensure that staff are aware of the need to comply with this policy and that appropriate records management practices are adopted. The DIGCs also support the work of CIGG by formulating action plans and escalating issues for further consideration.

- **Head of technology and change services** should inform the relevant DIGC and/or IAO of any systems migration and new procurements or developments of applications designed to store documents and records.

### Lifecycle of documents and records

All documents and records have a natural ‘lifecycle’ spanning from their creation to their subsequent disposal. During this lifecycle, they need to be maintained securely to ensure their accuracy, reliability and authenticity. The lifecycle for a document or record ends when there is no longer a business or statutory need for its retention.

#### Creation

The creator of a record or document should take into account the business, legislative and regulatory environment that applies to a particular task or activity and the purpose behind the document they are creating. An adequate record will provide full and complete evidence of a business process, including the consideration of the council’s business needs and statutory obligations.

All council employees must be able to distinguish between a record and other documentation they may hold. A record generally requires more active involvement to maintain its accuracy and reliability than other documents. Definitions of what is a record and what is a document are set out in Annex 1 to this policy.

#### Maintenance and use

All officers are responsible for ensuring any documents or records they use or have access to, whether paper or electronic, are kept secure and safeguarded from unauthorised access, alteration, corruption and accidental loss. They are also responsible for ensuring that the documents or records are accurate and up to date, and are stored and classified in a way that relates them to other records of a similar nature. Security measures should be applied as necessary. These will include:
• Being aware of the security marking status of a record;

• Using lockable storage cabinets for paper records which require an enhanced level of security;

• Using GCSx or Egress transmission methods for electronic records which require an enhanced level of security;

• Using approved transit methods or systems for the secure distribution or sharing of records; and

• Adopting systems to track the use or location of records.

Closure

When the purpose for which a record was created is complete, or when the record ceases to be in active use, it should be closed. A record should also not remain open indefinitely. A new record should be created if a clear break point is reached in the record’s lifecycle.

Closed records should be removed from use and stored securely. Paper records may be removed from working offices and placed in appropriate storage (including approved off-site locations). This is called ‘archiving’. Each information asset owner should identify suitable locations for the storage of closed files relating to each information asset. Electronic records may be archived by being collapsed or ‘zipped’ and moved to a new server location (on the council network) or saved to other electronic media (approved for use by technology and change services).

Archiving records helps to ensure that searches for live records are not cluttered or obstructed by obsolete records. It also ensures compliance with the principles of the Data Protection Act in respect of keeping personal data secure and only as long as necessary.

Closed records should be subject to a retention or deletion period, based on the council’s records retention and disposal schedule. The retention period begins at the date of closure.

Disposal

If there is no further business or regulatory need to keep a particular record, at the end of its retention period it must be authorised for disposal by the information asset owner and disposed of securely and confidentially.

All staff responsible for making decisions on the retention and disposal of records must do so in accordance with the council’s records retention and disposal schedule.
The schedule acts as a timetable for the review of records and documents stored by the council. The schedule applies to all records, documents, information and data processed by the council regardless of the format of the record. If a particular record or document does not fall into any of the categories in the schedule, advice must be sought from the information governance manager.

**Compliance**

All users of the council’s information resources are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the officers’ code of conduct and could result in disciplinary action being taken against the officer concerned.

**Review and revision**

This policy will be reviewed by the information governance manager annually. Any proposed changes to the policy will be considered by the corporate information governance group which is chaired by the SIRO.

**This policy was last revised in July 2015.**

**References**

This policy should be read in the context of the council’s other policies and guidelines in addition to national legislation, codes of practice and accepted best practice. In particular, this policy should be read in the context of:

- ISO15489: Parts 1 and 2. (2001): defines the systems required by an organisation to comply with records management obligations. We are committed to compliance with this standard.

The following council policy documents are directly relevant to this policy:

- Information governance policy
- Personal privacy policy
- Information access policy
Technical security policy

Section 14 of the finance manual

Key messages

1. Every council officer has a duty to ensure all data, available on any platform, is used, stored, and disposed of responsibly.
2. Documents and records should be easily accessible to officers who require them.
3. Officers should make sure they understand what security measures are applicable to each type of record.
4. All data breaches must be reported.
5. Officers should dispose of records in accordance with the retention policy.
6. Once the records are ‘closed’, physical materials should be archived and electronic data should be stored in the ‘archived shared folder’.

Annex 1: definitions

Records

A record is any recorded information in any format or media that the council creates, captures, collects, receives and/or uses to initiate, conduct and/or complete a council process or activity provide evidence of a particular activity or course of action and therefore they must be looked after to ensure they are accurate, trustworthy and protected from unauthorised alterations or deletion.

Records are defined as:

“information created, received, and maintained as evidence and information by an organisation or person in pursuance of legal obligations or in the transaction of business” (ISO15489-1:2001).

Some examples of records are:

- Final versions of reports, contracts, policies and council plans;
- Minutes of meetings kept by the meeting chairperson or administrator;
- Client case files; and
- Employee files.
Documents

A document may not carry the same evidential weight as a record but documents are important to our business. Some documents may only be needed for short term use and can be deleted or shredded as soon as their use is concluded.

Documents can be defined as:

“a named structural unit of text that can be stored, retrieved and exchanged among systems and users as a separate unit”.

Some examples of documents are:

- Draft or earlier versions of policies, plans and reports;
- Templates for adding information;
- Notes from meetings intended for personal use;
- Copies or duplicates of records;
- Items of post including email;
- Printed reprographics; and
- Any unit of text that can be communicated but does not then need to be retained as a record.

Records management

Records management is about the systems in place to look after records and exploit the value of information.

Records management is defined as:

“field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records” (Committee Draft International Records Management Standard 6, 1999).

Electronic documents and records management systems (EDRMS) offer organisations systematic control over documents and records throughout their lifecycle. These are repositories for documents and records that can apply access control, security marking, retention control and classification to records by use of metadata.