OPCC Records Management Policy

Document Approval and Identification

Author	Michael RICHMOND
Version Number	1.3
Date	27th March 2020

Version History

Version No.	Version Issue Date	Authored / Revision by	Approved by	Reason
1.0	**1/10/2018**	**Mike Richmond**	**Rachel Cook**	
1.1	**7/11/2019**	**Mike Richmond**	**Rachel Cook**	**Rewrite following ICO feedback**
1.2	**22/1/2020**	**Mike Richmond**	**Mike Richmond**	**Transferred into new format**
1.3	**27/3/2020**	**Mike Richmond**	**Mike Richmond**	**Updated for Pentana System**

Policy Statement

The Office of the Police and Crime Commissioner (OPCC) for Humberside is committed to create, keep and manage records which document its principal activities. The effective management of our records will enable us to comply with legal and regulatory obligations, preserve corporate memory and to manage our operations successfully.

Introduction

It is recognised that information is a vital asset of the Office of the Police and Crime Commissioner (OPCC) for Humberside, which depends on reliable, up-to-date information systems to support the work that it does and the services provided to the citizens of Humberside.

Scope

This policy cover business records. Not all documents are records. A record shall be considered to be "information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business". It includes some – but not all – business emails as well as meeting minutes, memoranda, employment contracts, and accounting source documents.

Aims and Principles

The aim of this Records Management Policy is to ensure that our records:

- provide authoritative information about past actions and decisions for current business purposes;
- protect the legal and other rights of the OPCC, its staff and its stakeholders i.e. what assets we hold;
- explain, and if necessary justify, past actions in the event of an audit, public inquiry or other investigation e.g. expenditure of public funds, handling of an FOI request.

The following documents support this policy:

- OPCC for Humberside Data Protection Policy
- Humberside Police Information Security Policy
- NPCC Review Retention and Disposal Schedule
- OPCC for Humberside Retention Policy

Relevant legislation:

- Freedom of Information Act 2000
- General Data Protection Regulations
- Data Protection Act 2018
- Environmental Information Regulations 1992 and Environment Information (Amendment) Regulations 1998
- Limitation Act (1980)

We will ensure that staff creating or filing records are aware of the need to give those records titles that reflect their specific nature and contents so as to facilitate retrieval. Where possible, records will be held electronically.

We will dispose of short lived material regularly – for example, print outs of electronic documents should not be kept after the meeting for which they were printed, trivial emails should be deleted after being read and keeping multiple or personal copies of documents is discouraged.

Roles and Responsibilities

All staff have a responsibility to ensure that information is appropriately managed. In addition, the roles listed below have specific tasks.

Senior Management Team – overall responsibility for the information management strategy and policy framework and for supporting its application throughout the organisation.

Data Protection Officer – responsible for ensuring policies, procedures and guidelines for good information management practice are in place, and for promoting compliance with these policies. Supporting the development of folder classification schemes, file plans and retention and disposal schedules.

All Staff – responsible for following policies and procedures for managing information. All staff also have a responsibility to protect sensitive and personal information. They must not disclose it to unauthorised parties or allow it to be transmitted or transported in an unsecure way. Further advice is provided in the Humberside Police Information security Policy.

Pentana Records

Pentana is the OPCC's Electronic Document and Record Management System (EDRMS). It is provided for the use of staff to store and manage their workflow and it can also store electronic records.

Records Creation

Only **business records** should be stored on Pentana. They should be given appropriate filenames and metadata to enable you or others to find and use them in the future.

What is a Business Record?

A business record is a document (hard copy or digital) that records a business dealing. Business records include meeting minutes, memoranda, employment contracts, and accounting source documents.

Emails

Emails are considered information under the terms of this policy and some emails will also be a business record. Emails which form a business record that need to be accessed and shared with other staff members should be saved in Pentana rather than folders in your inbox. This will ensure that they form a complete record with other associated documentation.

It is important that only essential business emails are saved to Pentana. Documents which may be attached to an email and need to be saved as a corporate record, must be saved to the shared drive, and not simply retained on an email. This will ensure they are available to all staff who need access to them.

Naming Conventions

Files should be named in accordance with the OPCC best practice guidance on file naming (Appendix A).

Metadata

Where Pentana asks for Metadata (further information about a file in addition to its filename) you should try to record as much information as possible. This further information helps us identify file types.

Security

Access to Pentana records is controlled by permissions linked to individual user logins. It is possible to share documents with other, appropriate members of staff. The preferred way to do this is through adding the person to the record's permissions in Pentana and not circulating the document on paper or by email.

Version Control
Pentana does not allow for version control; that is, it is possible to store multiple outdated versions of a record. Staff should therefore avoid uploading multiple copies of a document, to reduce the number of search "hits". Where multiple copies of a document are required – for example to keep a record of changed policies – version numbering as per the best practice guide (Appendix A) must be used to allow identification and use of the most up-to-date version of the record.

Review Retention and Disposal
Records that are no longer required must be disposed of in accordance with our Retention Policy. Where a record has been correctly uploaded to Pentana, the original copy – paper or electronic – does not need to be retained. By default, files that are uploaded to Pentana are kept for **six years** and then disposed of**.** If you need to change the retention period, the system will automatically flag files for you to review. It is important that you do so promptly to prevent them from being automatically deleted.

Manual Records

A lot of information OPCC staff handle will not be a business record; and not all business records will belong to the OPCC and need to be stored on our systems – for example, minutes of meetings that were chaired by other organisation will be managed by them, and need only be stored if they are relevant to the work of the office.

Some other types of records are not suitable for inclusion in the Pentana system. This includes records that must be stored in paper format, records that are too large to scan, records that are not business records but required for short-term projects. Such records still must be properly managed and are still disclosable under the Freedom of Information Act.

Manual records **must** be recorded in the Information Asset Register, which is held by the Data Protection Officer. This allows the organisation to identify records outside the Pentana system, for instance to identify them if a request is made under the Freedom of Information Act.

Paper Records

Paper records must be kept to a minimum. Secure storage facilities have been provided for staff with a business need to store paper records and they must be kept organised by that member of staff. Storing paper records outside of the approved cabinets may result in you breaking the organisation's information security policy.

Filing Systems

Information Asset Owners are responsible for organising the filing system for their paper records. Records **must** be organised in a way that allows you to retrieve them on-demand. The Data Protection Officer is able to offer advice if needed.

Security

A secure room has been provided for those staff with a business need to retain paper records. This consists of a filing cabinet drawer within a locked room. The room **must** be kept locked at all times when not in use and all records **must** be stored within a drawer. It is not permissible to store any other items in the designated file storage room.

Offsite Storage

Offsite storage facilities are available for certain business critical records. Records stored offsite are still our responsibility and the information asset owner will be required to manage their review, retention and disposal.

Review Retention and Disposal

Information Asset Owners are responsible for maintaining a review and disposal schedule for manual records. Advice on secure disposal is available from the Data Protection Officer but staff members must sift, sort and dispose of the records themselves, recording the reasons if a record is to be retained longer than the standard six-year period. All paper records **must** be reviewed at least every six years to ensure there is a lawful basis for their retention.

Manual Electronic Records

Naming Conventions

A document name or title is often the first point of identification, so it is crucial that this name will sufficiently distinguish it from other documents. Adopting some basic naming conventions will allow us to enable consistency in naming documents and assist in navigation and searching and allow a shared understanding of the content and context of a document's content.

Version Control

The use of version control can greatly assist with retrieving records quickly and accurately. It allow users to track a document's progress during drafting and/or review and revert to previous versions if needed. Version control can be achieved by:

- using a document control table at the beginning of a document (most useful for policies and records that tend to change over time)
- adding version numbering in the title of a record, in-line with the OPCC best practice guidance (Appendix A).

Security

Access to folders on the OPCC network is restricted on a “need to know” basis and secure folders are available for SMT members to store sensitive information. Access rights to folders are controlled by the Statutory Operations Manager.

Retention

Records that are no longer required must be disposed of in accordance with our Retention Policy. This is the responsibility of the information asset owner. All manual electronic records **must** be reviewed at least every six years to ensure there is a lawful basis for their retention.

Appendix A

OPCC for Humberside Guidance on Naming Conventions

Good file names are essential to accessibility. Please bear the following points in mind when naming any documents you have created:

1. Keep file names short but meaningful.

2. Avoid unnecessary repetition in file names.

3. Use capital letters or underscores (_) to delimit words not spaces.

4. If using a date in the file name always state the date 'back to front' and use four digit years, two digit months and two digit days: YYYYMMDD. Put the date at the beginning of the filename.

5. When including a personal name in a file name give the family name first followed by the initials.

6. Avoid using common words such as 'draft' or 'letter' at the start of file names, unless doing so will make it easier to retrieve the record.

7. Order the elements in a file name in the most appropriate way to retrieve the record.

8. The file names of records relating to recurring events should include the date and a description of the event (except where this would be incompatible with 2 above).

9. The file names of correspondence should include the name of the correspondent, an indication of the subject, the date of the correspondence and whether it is incoming or outgoing (except where this would be incompatible with 2 above).

10. The file name of an email attachment should include the name of the correspondent, an indication of the subject, the date of the correspondence, 'attach' and an indication of the number of attachments sent with the covering email (except where this would be incompatible with 2 above).

11. The version number of a record should be indicated in its file name by the inclusion of 'v' followed by the version number.

12. Avoid using special characters in file names.