Office of the Police and Crime Commissioner for Humberside

Records Management Policy

Policy Statement

The Office of the Police and Crime Commissioner (OPCC) for Humberside is committed to create, keep and manage records which document its principle 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.

A copy of this policy will be published on our website so that the public can see the basis on which we manage our records.

Compliance will be monitored periodically by the Governance and Administration Manager and the policy will be reviewed every 3-5 years.

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 ie what assets we hold;

- explain, and if necessary justify, past actions in the event of an audit, public inquiry or other investigation ie expenditure of public funds, handling of an FOI request.

Relevant legislation:

- Public Records Act 1958 and 1967
- Local Government Act 1972
- Freedom of Information Act 2000
- Data Protection Act 1998
- Environmental Information Regulations 1992 and Environment Information (Amendment) Regulations 1998

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 ie 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 should be 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 policy framework and for supporting its application throughout the organisation.

Governance and Administration Manager – responsible for ensuring policies, procedures and guidelines for good information management practice are in place, and for promoting compliance with these policies.

Administration Team – ensuring procedures are in place and the management of information is carried out in accordance with this policy and associated procedures. Maintaining 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.

Records Creation

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.

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 the relevant folder on the shared drive. This will ensure that they form a complete record with other associated documentation.

It is important that only essential business emails are saved to the shared drive. 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.

Retention

Records that are no longer required will be disposed of in accordance with our Retention Policy.