Not protectively marked

Office of the Police and Crime Commissioner – Devon & Cornwall

Policy Cover Sheet

Policy Name:	Records and Information management policy
Version Number:	V1.0
Date:	10/09/14
Policy Author:	Eleanor Tanner, Office Manager
Policy Authorised by:	Andrew White
Policy Sign off Date:	25 September 2014
Policy signed off by:	Andrew White, Chief Executive
EIA status	

Office of the Police and Crime Commissioner – Devon & Cornwall
Records and Information Management Policy

Version dated: 10/09/2014

1.0 Contents List [FOIA Open]

2.0 Policy Statement [FOIA Open]

2.1 The Office of the Police and Crime Commissioner is committed to the creation, retention and management of records which document the principal activities of the organisation and that meet business needs, accountability requirements and stakeholder expectations. In addition, the Office of the Police and Crime Commissioner is committed to the principles and practices set out in the whole of Government policies and best practice standards.

3.0 Purpose and scope [FOIA Open]

3.1 The purpose of this policy is to provide guidance and direction to the creation and management of information and records and to clarify staff responsibilities.

3.2 Information is the basis on which decisions are made and policies developed and communicated. Information, like other assets, needs to be classified, structured, validated, valued, secured, monitored, measured and managed. This policy and associated policies and supporting documents aim to ensure that the organisation's records and documents which are critical to the activities of the Police and Crime Commissioner and his / her office are managed in accordance with legislative requirements and best practice so

that information can be found when requested, and can be relied on as authoritative.

3.3 The Office of the Police and Crime Commissioner will implement fit-for-purpose information and records management practices and systems to ensure the creation, maintenance and protection of reliable records. All information and records management practices in the Office of the Police and Crime Commissioner are to be in accordance with this policy and its supporting procedures.

3.4 The policy applies to all staff within the Office of the Police and Crime Commissioner, and to agency, associated and affiliated workers. It incorporates all relevant documents and records (recorded information) throughout their life, from planning and creation through to disposal, whatever the medium or technology used to create and store it and whether it originates from within the organisation or from outside. It also covers documents and records stored on behalf of the Office of the Police and Crime Commissioner by an external body (for example the Police Force).

3.5 The benefits of being in control of our records and information include:

- Information can be found by the right people, for the reasons required and in a timely manner.
- Information can be opened by the right people for the right purposes.
- Information can be worked with in the appropriate manner, including transfer to other organisations and disposal
- Information can be trusted in that it is what it purports to be and that there is a suitable history of when the information has been changed.
- Information can be understood in terms of both its business purpose and what it relates to.

3.6 The risks of poor records and information management include:

- Poor decisions based on inaccurate or incomplete information
- Financial or legal loss if information required as evidence is not available or cannot be relied upon.
- Non-compliance with statutory or other regulatory requirements.
- Failure to handle confidential information and possibility of unauthorised access or disposal.
- Failure to protect vital information that enables the continued functioning of the organisation leading to inadequate business continuity planning
- Wasted time on searches
- Loss of reputation and damaged public trust.

3.7 All staff are under a statutory obligation to create accurate records of their activities and to manage and maintain such documentation in accordance with this policy, and associated policies and supporting documents. Any departure from this may lead to disciplinary action being taken in accordance with the published staff disciplinary process.

3.8 This policy is supported by the following complementary policies and additional guidelines and procedures:

- Information Retention and Disposal Policy and Schedules
- Information Security Policy
- Data Protection Policy
- Freedom of Information Policy
- Risk Management Framework
- Memorandum of understanding for the processing of data
- Guide to using the 'Office of the PCC' Corporate e-Filing System

3.9 Definitions

Documents -*a* document can be defined as information stored as a single entity on some medium e.g. paper or computer drive.

Records - a record can be defined as a document which has content, context and structure and contains 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'. [International Standards Organisation ISO 15489 Information and documentation: Records management, two volumes 2001]*

Records derive from documents, all records will be documents, but not all documents will be records.

Records / document management – records / document management can be defined as managing records / documents within a file system (electronic and / or paper) including classifying, capturing, storing and disposal.

4.0 Legal and regulatory environment [FOIA Open]

4.1 The organisation has a responsibility to comply with legal or statutory regulations and records and information must be managed to fulfil these responsibilities. The key legal and regulatory obligations that are either directly relevant to, or have a strong influence over the organisation's arrangements for information and records management include:

Freedom of Information Act 2000, and the Lord Chancellor's code of practice on management of records issued under section 46 of the FOI Act 2000 – the duty to follow the code in connection with the keeping, management and destruction of records.
Data Protection Act – the duty to comply with the data protection principles.
Environmental Information Regulations – the duty to comply with rights of access to environmental information.
Accounts and Audit (England) Regulations 2011-the duty to record up to date accounting records.
Public Sector information Directive and Regulations - encourages the re-use of public sector information by removing obstacles that stand in the way

of re-use. The main themes are improving transparency, fairness and consistency.

Management of Health and Safety at work Regulations 1999 (regulation 5) – the duty to record health and safety arrangements

Police Reform and Social Responsibility Act (Section 36)

- the duty for the police force and Police and Crime Commissioner to share financial information, in particular for the Police and Crime Commissioner to have full access to all relevant financial information.
- the duty to publish information considered necessary to enable the local public to assess their performance and that of the Chief Constable.
- the duty to publish information as specified in the Elected Local Policing Bodies (Specific Information) Order 2011 and in regulations issued under section 11 of the Police Reform and Social Responsibility Act 2011.
- the duty to deliver value for money, enabled by data that is fit for its intended purpose, and are used and published routinely, providing a clear line of sight between consumption of resources, production of outputs and realisation of outcomes.

Local Audit and Accountability Act 2014 – the duty to provide documents and information to the auditors, which it appears necessary to enable them to discharge their functions under the Act.

5.0 The role of records and document management and the relationship to the Police and Crime Commissioner's overall business strategy. [FOIA Open]

5.1 Available and authoritative information is an asset that is essential to the work of the organisation. It will enable:

- The Police and Crime Commissioner to deliver on his / her responsibilities as defined in the Police Reform and Social Responsibility Act.
- The Police and Crime Commissioner to deliver on his / her promises as defined in the police and crime plan.
- Legal decisions to be made that are defendable when challenged.
- Policy making.
- The fair allocation of funds through commissioning activity.

6.0 Creation and maintenance of information and records [FOIA Open]

6.1 Business information and records must be created and captured by everyone subject to this policy. Business information and records created should provide a reliable and accurate account of business decisions and actions, include all necessary information to support business needs including names, dates and times, and other key information needed to capture the business context.

6.2 The types of information and records that need to be created, captured and managed to support the organisational business and legal requirements include, but are not limited to:

- All information that is required to be kept by legislation or regulation.
- All information that provides an authoritative record about past actions and decisions for current business purposes.
- All information needed to protect the legal and other rights of the organisation and its staff and stakeholders.
- All information that will explain or justify past actions in the event of an audit, public enquiry or other investigation

6.3 All business information and records created and received should be captured into endorsed information and records systems.

6.4 The record and information retention and disposal policy and schedules, and the corporate filing system management rules should be read in conjunction with this policy. These documents provide further guidance on titling documents and records, when and where to capture information and records and rules for retaining and disposing of information and records.

7.0 Systems used to maintain information and records [FOIA Open]

7.1 The Office of the Police and Crime Commissioner's primary information and records management system is the Corporate e-Filing System, a hierarchical filing structure stored on the shared computer drive using Microsoft Windows.

7.2 Where possible, all incoming paper correspondence received by the organisation will be converted to digital format and saved into the Corporate Filing System. In limited circumstances, such as for particular security purposes, there may be a requirement for paper files to be created. The Office Manager will be consulted in these instances.

7.3 The following business and administrative databases and software applications are also endorsed for the capture and storage of specific information and records. These include:

- SharePoint
- Covalent
- OPCC Contact Database
- OPCC Website
- Agresso

7.4 Corporate records will not be maintained in email folders, shared folders, personal drives or external storage media as these lack the necessary functionality to protect business information and records over time. Records created when using social media applications or mobile devices may need to be captured into an endorsed system.

8.0 Access to records and information arrangements [FOIA Open]

8.1 Legislation such as the Elected Local Policing Bodies (Specified Information) Order 2011, the Freedom of Information (FOI) Act 2000 and Environmental Information Regulations and the Data Protection Act provide for public access to records and information held by the Office of the Police and Crime Commissioner, subject to certain exemptions.

8.2 In accordance with our obligations and in the spirit of transparency, access to publicly available information will be provided on our website. The Publication Scheme provides further details of records and information that are routinely published.

8.3 Decisions to restrict access to records and information to members of the public will be in accordance with the relevant legislation. Operational responsibility for this function has been allocated to the Office Manager, who is also responsible for compliance.

8.4 Information and records are a corporate resource. One of the primary objectives of information management is to ensure appropriate access to information such that information can be opened by the right people for the right purposes. Access to organisational information by internal stakeholders will only be restricted where there is a legal or organisational reason for doing so. Access restrictions will not be imposed unnecessarily, but will be applied to ensure the proper protection of the privacy of individuals.

8.5 Decisions to restrict access to information will be taken by the Office Manager where there is a legal or regulatory requirement to restrict access, and by the Chief Executive where there is an organisational reason for restricting access.

8.6 This policy should be read in conjunction with the Information Security Policy, Freedom of Information Policy, and Data Protection Policy which specifically cover access to data and information.

9.0 Retention or destruction [FOIA Open]

9.1 Some records and information can be destroyed in the normal course of business. These are records of a short-term, facilitative or transitory value that are destroyed as a normal administrative practice. Examples of such records include rough working notes, drafts not needed for future use or copies of records held for reference.

9.2 All other records and information have an allocated retention period and will be maintained or disposed of in accordance with the Information Retention and Disposal Policy and Schedules which can be located here.

9.3 All staff, agency, associated and affiliated workers should be familiar with the policy and be aware that unauthorised destruction not only risks penalties under the Freedom of Information Act but may expose the organisation to a range of other risks including:

- an inability to comply with regulatory and legislative responsibilities

- damage to organisational reputation.

9.4 No-one should destroy records, other than in accordance with the Information Retention and Disposal Policy, without the approval of the Chief Executive. Furthermore, records should not be disposed of if they are the subject of a current or pending enquiry, which may be under the Freedom of Information Act, Data Protection Act, or other enquiry including internal investigations. Staff can be held personally liable for unauthorised destruction.

10.0 PCC records and documents held by other organisations [FOIA Open]

10.1 Certain records and documents that relate to the Office of the Police and Crime Commissioner's functions and activities are held by the Police Force, or stored on externally-hosted electronic systems, e.g. Agresso and Covalent.

10.2 The ownership of records and documents that are stored on outsourced, contracted storage and retrieval facilities, and / or externally-hosted electronic systems remain under the ownership of the organisation.

10.3 The proper management of the organisation's information assets regardless of where they are held, and how they are held, is essential to the business continuity of the organisation. Therefore the principles of records and document management detailed in this policy, apply to all records and documents that fall under the ownership of the organisation.

10.4 The Office Manager will represent the requirements of the Office of the Police and Crime Commissioner on the Police Force Information Strategic Group, and it will be through this forum that the organisation will ensure that those records and information held by the Police Force on behalf of the Office of the Police and Crime Commissioner, are managed in accordance with this policy, and maintained in a format that satisfies the requirement that records must be accessible over time regardless of what medium they are stored on.

11.0 Governance framework including roles and responsibilities [FOIA Open]

11.1 Information and records are corporate assets and loss of the asset could cause disruption to business. For this reason, records and information management is incorporated and explicitly recognised within the corporate risk register. The level of risk will vary according to the strategic and operational value of the asset to the organisation and risk management will reflect the probable extent of disruption and resulting damage. Mitigation includes mechanisms to ensure that any proposed structural, organisational or financial changes are subject to a risk assessment review in terms of their likely impact on the records and information management function.

All Employees

11.2 It is the general responsibility of officers to document their work in the way that the Police and Crime Commissioner has specified, and in accordance with legislation, and to use those records appropriately including the maintenance and disposal of records and documents.

Chief Executive

11.3 The CEO is ultimately responsible for the management of information and records within the Office of the Police and Crime Commissioner. The CEO has authorised this policy. The CEO promotes compliance with this policy, delegates responsibility for the operational planning and running of information and records management to an appropriate officer in the organisation and ensures the organisation's information and records program is adequately resourced.

Chief Executive and Treasurer

11.4 Executive officers are responsible for the visible support of, and adherence to, this policy by promoting a culture of compliant information and records management within the organisation and contributing to the development of information and records management strategic documents.

Office Manager

11.5 The Office Manager is responsible for overseeing the management of information and records in the organisation consistent with the requirements described in the policy. This includes providing training, advice and general support to staff, creating, developing or acquiring and implementing information and records management products and tools, including systems to assist in the creation of complete and accurate records, developing and implementing strategies to enable sound records management practices, monitoring compliance with information and records management policies and directives and advising senior management of any risks associated with non-compliance.

Managers

11.6 Managers and supervisors are responsible for ensuring staff, including contract staff, are aware of, and are supported to follow, the information and records management practices defined in this policy and supporting standards, procedures and guidelines. They should advise the Office Manager of any barriers to staff complying with this policy. They should also advise the Office Manager of any changes in the business environment which would impact on information and records management requirements, such as new areas of business.

Contract staff, agency, associated and affiliated workers

11.7 Contract staff, agency, associated and affiliated workers should create and manage records in accordance with this policy.

12.0 Communication and Training [FOIA Open]

12.1 This policy will be communicated to all staff, contractors, agency, associated and affiliated workers as appropriate, and training will be provided on aspects of the policy. The training will be up to date, regular, and tailored to workgroups as appropriate.

13.0 Supporting documents [FOIA Open]

13.1 This policy is supported by information retention and disposal schedules and information management rules, which comprise the following processes:

- Creation and Capture/Receipt of Information
- Storage and Retrieval of Information
- Dissemination of Information
- Retention and Disposal of Information

14.0 Monitoring and review [FOIA Open]

14.1 This policy will be updated as needed if there are any changes in the business or regulatory environment. It is scheduled for a comprehensive review by 2017. This review will be initiated by the Chief Executive and conducted by an internal committee of senior management.

14.2 The Chief Executive, line managers and individuals each have responsibility in ensuring the successful and consistent delivery of this policy, and supporting standards, procedures and guidelines.

14.3 Compliance with this policy will be monitored by the Office Manager (with the support of workplace Managers). Levels of compliance will be reported at least annually to senior management.

15.0 Audit Compliance [FOIA Open]

15.1 This policy has been drafted and audited to comply with the principles of the Human Rights Act. Equality and diversity issues have also been considered to ensure compliance with equality legislation and policies. In addition Data Protection, Freedom of Information, Management of Police Information and Health and Safety issues have been considered. Adherence to this policy will therefore ensure compliance with all relevant legislation and internal policies. Under the Freedom of Information Act 2000, the document is classified as 'OPEN'.

16.0 Ownership [FOIA Open]

16.1 This policy is owned by the Office of the Police & Crime Commissioner.

17.0 Useful Links [FOIA Open]

- Data Protection Policy

- Information Security Policy
- Freedom of Information Policy
- Information Retention and Disposal Policy and Schedules
- Information sharing policy
- Risk Management Framework
- Memorandum of Understanding for the processing of data between the OPCC and the Devon and Cornwall Police *(pending 10/09/14)*
- Guide to using the 'Office of the PCC' Corporate e-Filing System