OFFICE OF THE POLICE AND CRIME COMMISSIONER

INFORMATION MANAGEMENT AND SECURITY POLICY

Introduction
The Office of Police and Crime Commissioner (OPCC) for Northumbria is committed to the highest possible standards of openness, probity and accountability. All organisations generate records which must be collated, maintained and revised over time. As a public body the office of the police and crime Commissioner for Northumbria has a responsibility to be accountable to the public for their actions. Therefore the records must be accurate and capture the correct details of transactions. The policy for management of these must protect the rights of privacy, confidentiality and security. This applies to the management of records of all formats or media, whether created or received.

Effective records management is essential to the support compliance with the Freedom of Information Act 2000, FOIA, the Section 46 Records Management Code issued under the Data Protection Act (DPA) 1998.

This policy statement sets out the OPCC for Northumbria manages information and complies with its statutory obligations and will be kept under annual review. It applies to all the information held by the office, regardless of its format or origin. It includes policy and procedures around:

- Records management, security and sharing information; and
- Retention and destruction of documents.

The Data Protection Act
The DPA 1998, tries to strike a balance between the rights of individuals and the needs of organisations wanting to use their personal information The DPA places obligations on those who process data while giving rights to those who are the subject of the data. Personal information includes both facts and opinions about the individual.
There are eight principles of good practice in handling personal information properly.

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept longer than necessary.
- Processed in accordance with the individuals rights.
- Secure.
- Not transferred to other countries without adequate protection.

There are special arrangements under the Act for processing sensitive personal information. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sexuality, criminal proceedings or convictions.

The Freedom of Information Act
The FOIA provides individuals or organisations with the right to ask for information held by the OPCC. They can do this by letter or email. The public authority must tell the applicant whether it holds the information, and must supply it within 20 working days, in the format requested. The OPCC does not have to provide information if an exemption applies, or in certain cases if the cost of providing the information is too high. The Act applies to all information, not just information held since the Act came into force.

Records Management and Information Security

All organisations generate records which must be collated maintained and revised over time. Public authorities are accountable for their actions to the public so need to ensure their records are accurate and reliable. A record is any report, letter, email, minute, decision mote, meeting note or other document whether hard copy or electronic, whether created or received and includes any personal data.

The OPCC approach to record management aims to ensure that:

- The value of information is understood;
- Records are present;
- Records can be accessed easily;
- Records can be easily interpreted;
- Records are a reliable representation of that which it is supposed to document; and
- Qualities of the document can be maintained, despite alterations or adaptations over time.

The OPCC is committed to the creation, storage, management and eventual disposal of records in a manner accurately documenting the functions of the OPCC and compliant with this policy. All staff who create, receive and use records have record management responsibilities at some level.

The OPCC will ensure that it develops and utilises systems for the documenting of its activities and registering its records. In order to maintain records efficiently and where applicable, there should be a tracking system in place so the location of particular records can be established and retrieved.

Our policy is to:

- Manage information effectively as a strategic corporate body by providing timely, appropriate, accurate and up-to-date information when it is needed;
- Make information available to those with a business need to see it;
- Take appropriate measures to protect information, including personal information, which cannot be shared for reasons of security or privacy;
- Assess and manage risks to the confidentiality, integrity and availability of information;
- Ensure that information created, collected and stored is proportionate to the business need, and is retained only for as long as it is needed;
- Ensure information is of the appropriate quality, and in the appropriate media, to support business needs;
- Create an information literate culture, where all staff recognise that information is everyone's responsibility and have the skills, confidence & commitment to effectively manage information according to the requirements of their role; and
- Comply with all relevant statutory and regulatory requirements; and

Electronic records

Electronic records will be held in structured folders with logically group information together with security arrangements to ensure the integrity of the records can be maintained and protected from loss or destruction. It should be remembered that it may be necessary for electronic records to be transmitted from one system to another and their format should be consistent with this.

Information Security

All employees should report any breach, possible breach or threat of any sort, to the security of OPCC information systems. Information is not just data contained on computer systems, it is any information, whether audio, video, CCTV, desk diaries or indeed any paper system. This should be done via line management or by the use of confidential reporting

Mobile Working and Transportation of Data

All devices containing OPCC data must be safe and secure when unattended both in and outside of the office. Information contained on a mobile device and taken off-site should be kept to a minimum.

Our policy is to:

- discourage unnecessary requests to transport sensitive data away from the main office and to seek clarity on the destination and proposed use of the information;
- ensure all documents are clearly marked 'confidential' where appropriate, and conceal paper documents from sight at all stages of the journey;
- provide secure external media devices (pen-drives, hard drives) to facilitate the need to transport sensitive data;
- ensure all staff are aware of their responsibilities when transporting data from one location to another; and
- ensure staff immediately report any loss of information to their line manager, in the first instance, or Chief Executive if out of office hours.

E-mail

Information that is passed over an insecure network should be considered as being open to the public. Therefore information which is not suitable for the public domain should not be processed or stored on personal computing equipment. Material marked as 'Restricted' or 'Confidential' should not be sent electronically to personal, unsecure email addresses.

The OPCC electronic system is delivered by Northumbria Police and procedures will reflect the requirements outlined in Northumbria Police's Operational Information Management Strategy.

Passwords

All staff have a responsibility for managing their own passwords and should not share passwords with others. Password should be changed regularly but not sequentially.

Government Protective Marking Scheme

Northumbria Police uses the Government Protective Marking Scheme (GPMS) and every document from them is marked '*Not Protectively Marked' / Protect / Restricted / Confidential / Secret / Top Secret'*. This policy advocates that the same markings scheme is adopted for information assets created by the OPCC for Northumbria.

In deciding the correct marking for the information, the initiator should consider how damaging the consequences would be if the material was lost, stolen, disclosed or destroyed.

Securing your PC

Where staff have to leave their desks in the office unattended they should press Ctrl-Alt-Delete together to lock their PC or log out of all systems. For a meeting or similar period of absence PC monitors should be also switched off.

Review

The OPCC undertakes to regularly review as appropriate, but no less frequently than every twelve months, its records management procedures to ensure compliance with this policy statement and to incorporate changes where necessary.

Retention and Destruction Procedure and Schedule

The OPCC is committed to operating in an open and transparent manner. The record disposal procedure is designed to support the Commissioner's corporate governance framework. The purpose of this procedure is to:

- prevent the premature destruction of records
- provide consistency of preservation/destruction
- improve record management

Records will be retained for the periods shown in the attached schedule (Appendix A). All retention periods are given in whole years and are from the end of the financial year to which the records relate. Records should be disposed of by shredding / arranging for collection as confidential waste for destruction by the appropriate body and this should also include all back-up copies on alternative media.

Litigation: Whenever there is a possibility of litigation or a request under the Freedom of Information Act the records that are likely to be affected should not be amended or disposed of until the threat of litigation has ended or the appeal processes under the Freedom of Information Act have been exhausted.

Record of Disposal: A record of disposal of the information detailed in the attached schedule should be maintained which identifies each record destroyed.

Standard Operating Procedure: This applies to records which do not need to be kept at all. Information which is duplicated, unimportant or of short term use can be destroyed under the Standard Operating Procedure, including:

- compliment slips;
- catalogue and trade journals;
- telephone message slips;
- non acceptance of invitations;
- trivial e-messages or notes not related to OPCC business;
- working papers which lead to a final report (including notes of meetings);
- duplicated and superseded material such as stationary, manuals, drafts, address books and reference copies of annual reports.
- e-copies of documents where a hard copy has been printed and filed or vice versa.

Except where these may be used as evidence to prove that something has happened.

DOCUMENT RETENTION PERIODS (APPENDIX A)

POLICE AND CRIME COMMISSIONER			
Function	**Records**	**Retention**	
A	Notes of meetings	Minutes, agendas and reports Rough/draft/audio minutes	Permanent Destroy on completion of final minutes/notes
B	Decisions	Decision reports Decision logs	Permanent Permanent
C	Partnership, agency and external meetings (where the Commissioner owns the record)	Minutes Agendas and reports	Permanent
D	External meetings (where the Commissioner does not own the record)	Minutes Agendas	3 years
E	Working Groups/Steering Groups/Review Groups	Minutes Agendas and reports	5 years
F	Appointment of Chief Constable	Advertisements Application forms Interview reports Personnel files	5 years 6 years from date of last pension payment
G	Dismissal of Chief Constable	Resignation, redundancy, dismissal, death, retirement	6 years after termination or, if pension paid, 6years after last pension payment
H	Complaints against Chief Constable	Correspondence	6 years after finalisation
I	Complaints - other	Correspondence Summary reports Details of investigations into complaints	6 years after finalisation 6 years after finalisation 6 years after finalisation

MEMBERSHIP			
Function	**Records**	**Retention**	
A	Appointment of members (Audit Panel, Scrutiny Panel and IAGs members)	Personnel files Application forms, interview notes,	Permanent 4 years after date of appointment
B	Attendance records	Attendance database	Permanent
C	Payments	Attendance allowance payment details	6 years after leaving
D	Registers of Members interests and hospitality	Register of Interests Register of Hospitality	Permanent
E	Personal Development Review	PDR – notes of meetings and records of development	5 years

MANAGEMENT AND ADMINISTRATION			
Function	**Records**	**Retention**	
A	Policy development	Policies Instructions/procedures Organisation charts Standing orders/financial regulations	Permanent
B	Policy / strategy review	5 years	
C	Public consultation	Notes, records, correspondence	3 years
D	Information management	Filing indices Records of transfer to archives Summary of responses to enquiries Disposal records	Permanent 12 years 6 years 2 years

		Reports/correspondence on disclosure decisions Routine responses to enquiries	
E	Media relations	Media reports Press releases	3 years 3 years
F	Marketing	Developing and promoting events Information about the PCC	2 years When superseded
G	Office Management	Contracts with suppliers	12 years from end of contract
H	Diaries and calendars	Electronic and manual diaries/calendars	3 years
I	Management Team notes		5 years

HUMAN RESOURCES			
Function	**Records**	**Retention**	
A	Personnel administration	Establishment lists Personnel files	Permanent Destroy 6 years from date of last pension payment/leaving date
B	Employee relations	Agreements Correspondence re. Formal negotiations Correspondence re minor & routine matters	Permanent 2 years
C	Disciplinary & grievance investigations (proved)	Disciplinary records	Oral warning – 6 mths Written warning – 1 year Final warning – 18 mths
D	Disciplinary & grievance investigations (unproved)	Disciplinary records Grievance records	Destroy immediately after appeal
E	Grievances	Correspondence and notes	6 years

F	Medical records	Medical examinations Adjustment to work examinations	75 years after DOB
G	Recruitment	Advertisements, application forms, references, interview reports	1 year after appointment made
H	PDR	Probation reports Performance reports & plans	5 years after action completed
I	Staff leave monitoring	Sickness records	2 years after action completed

FINANCIAL MANAGEMENT			
Function	**Records**	**Retention**	
A	Annual reports	Annual statement of accounts	Permanent
B	Internal Audit	Internal Audit Reports- main financial & subsidiary systems Value for money studies Working papers Follow up audits Reports/papers used in the course of a fraud investigation	Destroy on completion of next full audit Destroy on full implementation of recommendations or completion of follow up audit Destroy on completion of next full audit 6 years after legal proceedings are complete
C	Finance reports	Quarterly budget reports Working papers and system reports	Destroy when admin use complete
D	Approvals/purchase	Purchase/sales order	Destroy 7 years after end of financial year

E	Expenditure	Invoices/receipts Bank statements Vouchers/ledger	Destroy 6 years after end of financial year
F	Payroll	Claim forms Pay / tax records Summary pay reports	Destroy 7 years after the end of the financial year Destroy after admin use
G	Budget setting	Final annual budget Draft budgets and estimates Quarterly budget reviews	Permanent Destroy 2 years after budget set Destroy after following years budget adopted
H	Asset monitoring & maintenance	Asset registers	Destroy 7 years after the end of the financial year

ESTATES AND PROPERTY MANAGEMENT			
Function	**Records**	**Retention**	
A	Property acquisition	Plans and reports	Life of property plus 12 years
B	Property disposal	Survey reports Tender documents Conditions of contracts	Destroy 25 years after all obligations end
C	Management of buildings of special interest	Project specs Plans Certificates of approval	Permanent
D	Insurance	Insurance policies Correspondence	Destroy 7 years after terms expire

LEGAL SERVICES			
Function	**Records**	**Retention**	
A	Litigation	Correspondence Criminal and civil case files	7 years after last action
B	Advice	Correspondence	3 years
C	Agreements	Service level agreements with WYP	6 years after agreement expires
D	Contract development (ordinary)	Tender specification	6 years after terms have expired
E	Contract development (under seal)	Tender specification	12 years after terms have expired
F	Tenders	Tender envelope	1 year after start of contract
G	Evaluation of tenders (ordinary)	Evaluation criteria Successful tender document	6 years after terms have expired
H	Evaluation of tenders (under seal)	Evaluation criteria Successful tender document	12 years after terms have expired
I	Post tender negotiation	Minutes Correspondence	1 year after terms of contract have expired
J	Asset acquisition/disposal (non-land, Estates and Property Management)	Legal docs relating to purchase/sale Leases Tender documents	Destroy 6 years if under £50,000 Destroy 12 years if over £50,000

GENERAL			
Function	**Records**	**Retention**	
A	Health & safety	Risk assessments Accident books/RIDDOR correspondence and fire certificates	Destroy after 6 years
B	Government Department circulars	Statutes APA Circulars	Destroy after 3 years