



**RECORDS MANAGEMENT**  
**POLICY**

<b><u>Document Control</u></b>	
Version Number	1.0
Author (Name, Job Title)	Joanne Regan, Head of Assurance and Compliance
Date Approved	4 <sup>th</sup> May 2020
Approved By	Sian Curley, Chief Executive
Superseded Version	0.4
Date of Next Review	May 2024

## Version Control

<b>Version</b>	<b>Date</b>	<b>Amended By</b>	<b>Reason for Issue/Amendment</b>
0.1	16/02/17	Joanne Regan, Information Officer	New policy drafted to ensure GDPR compliance
0.2	26/10/17	Joanne Regan, Information Officer	Amendments after further research and consultation with the Chief Executive
0.3	12/01/18	Michelle Vaisey- Baker, Business and Finance Officer	Amend Chief of Staff to Chief Executive
0.4	29/04/20	Joanne Regan, Head of Assurance and Compliance	Policy reviewed to reflect updated retention and disposal policy and schedule and to improve readability. Sent to Chief Executive for comment.
1.0	04/05/20	Joanne Regan, Head of Assurance and Compliance	Minor amendments made after consultation with Chief Executive and content page added – policy approved.

# OFFICE OF THE POLICE AND CRIME COMMISSIONER

## RECORDS MANAGEMENT POLICY

### 1. Introduction

- 1.1 Effective records management is essential to support compliance with the Freedom of Information Act 2000 (FOIA), the Section 46 Records Management Code of Practice (the Code) issued under the FOIA and the Data Protection Act 2018 (DPA).
- 1.2 The Records Management Policy, along with the Retention and Disposal Policy and Schedule, provides guidance in relation to the management of the records generated or obtained by the Office of the Police and Crime Commissioner for Gwent (OPCC), ensuring that relevant legislation is adhered to.
- 1.3 This policy applies to all employees including the Police and Crime Commissioner (PCC) and Deputy Police and Crime Commissioner, contractors, consultants and volunteers undertaking OPCC business.

### 2. Aim

- 2.1 Records management is the process by which an organisation manages all aspects of records and information, from their creation through to their eventual disposal (Records Lifecycle). The aim of the policy is to ensure:
  - **Accountability** – records fully account for all business actions and decisions
  - **Accessibility and Security** - records can be located when needed and only those with a legitimate right can access the records and the information within them is displayed in a way consistent with its initial use, and the current version is identified where multiple versions exist.
  - **Quality** – records are complete and accurate and can be trusted
  - **Maintenance** – that the quality of the document can be maintained despite any alterations or adaptations over time
  - **Retention and Disposal** – records are retained and disposed of appropriately and those of historical interest, kept permanently with consideration given to archiving with Gwent Archives
  - **Staff Awareness** – all staff are aware of the responsibilities regarding records management

### 3. Definition of a Record

- 3.1 Records are defined in the Code 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.’

3.2 The Code also makes it clear that application applies to all records:

'It includes therefore not only paper files series and digital records management systems but also business and information systems (for example case management, finance, and geographical information systems) and the contents of websites.'

#### **4. The Need for Records Management**

4.1 There are a number of pieces of legislation which relate to the effective management of the OPCC's records, including:

- The FOIA - this provides a statutory right of access to information held by public bodies (subject to exemptions). There is an associated Code of Practice on Records Management with which public bodies are obliged to comply.
- The General Data Protection Regulation (GDPR) & DPA 2018 - this entitles individuals access to their personal information which is being processed by an organisation upon request.
- The Public Records Act 1958 and 1967 (PRA) - this ensures that all records are subject to effective management systems.

4.2 There are also a number of organisational policies (both specific OPCC and adopted policies from Gwent Police) that relate to Records Management, these include but are not limited to:

- Record Retention and Disposal Policy and Schedule;
- Breach Reporting Procedure
- Information Security Policy
- Business Continuity Management
- Joint Risk Management Policy
- Freedom of Information Policy

4.3 Failure to follow the Code may mean that the OPCC also fails to comply with other legislation concerning the creation, management, disposal, use and re-use of records and information and we may therefore be in breach of our statutory duties.

4.4 Effective records management will enable the OPCC to:

- make better use of space and storage facilities, both physically and electronically;
- make better use of staff time;
- have improved control over records;
- comply with legislation, best practice and other OPCC policies; and
- reduce costs

## **5. Responsibility for Records Management**

- 5.1 It is the role of the Chief Executive of the OPCC to endorse this policy, support the resultant policies and provide resources. The Head of Assurance and Compliance (HoAC) will have a duty to ensure that the OPCC complies with the legislation concerning records management.
- 5.2 The HoAC will be designated as taking the lead role and will be responsible for the function of records management. The OPCC will appoint/designate staff to assist with this function and they shall have appropriate skills and receive relevant training. All staff who create, receive and use records will have records management responsibilities at some level.
- 5.3 File lists are in use to manage both electronic and hard copy information. The file list for all electronic information kept on the shared drive used by all OPCC staff is periodically updated by the Administration. There is minimal information kept in hard copy format within the OPCC but where it is, the title and location of the copy is kept on a spreadsheet. This is also reviewed and updated periodically by the Administration Assistant.
- 5.4 Each area of work as identified on the retention and disposal schedule and the Information Asset Register has an allocated 'owner'. It will be this person's responsibility to ensure the information within their allocated folders is managed on a day-to-basis in line with this policy and with the Record Retention and Disposal Policy and Schedule.

## **6. Retention/Disposal of Records**

- 6.1 Disposal of records will take place in accordance with the Retention and Disposal Policy and Schedule. This Schedule has been compiled to meet all statutory obligations of the OPCC.
- 6.2 Once records are selected for disposal in accordance with the Schedule the method of disposal should be appropriate to the confidentiality of the record. Where documents are disposed of, then this should be done in a secure manner and a record should be kept, containing the reference, a description and the date of destruction.
- 6.3 When destroying a hard copy record, checks must be undertaken to ensure the digital record (if it exists and if appropriate) is also deleted and vice-versa. Destruction/deletion of both records must be recorded appropriately.
- 6.4 All records should be accurate and not kept longer than is necessary.
- 6.5 Where a record which is due for destruction becomes the subject of a request for information then destruction should be delayed until the request has been satisfied or, in the case of a refusal, until any complaint and appeal mechanisms have been exhausted. However, before a request for information has been received routine amendments or even deletion can take place.

6.6 Short-lived material will be disposed of regularly, for example, printouts 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 versions of documents will be discouraged.

## **7. Electronic & Hard Copy Records**

7.1 Effectively managing electronic records will require the maintenance of structured folders which logically group information together as well as ensuring the appropriate security arrangements are in place to ensure that the integrity of the records can be maintained.

7.2 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.

7.3 All electronic documents are to be saved on the shared drive which is accessible to all staff. Staff are discouraged from using personal drives and the hard drive of their computer as information saved in these locations is not accessible for the purposes of FOI.

7.4 Wherever possible electronic storage of information will be undertaken by means of scanning and hard copies disposed if appropriate.

7.5 Regular back-up of electronic information will be undertaken by the Shared Resource Service.

7.6 All staff will be discouraged from printing information unless it is essential for them to do so.

7.7 Original hard copies of certain information will be kept where the wet signature is required. Documents will include, but are not limited to, decision registers and signed monitoring reports.

## **8. Naming Electronic Records**

8.1 Record naming is an important process in records management and it is essential that a unified approach is undertaken across the OPCC to aid in the management of records.

8.2 In constructing a title it is necessary to decide how best to describe the content of the file or the individual document. The most commonly used elements in the creation of a title are listed below. It will depend on the nature of the document or folder which elements will be the most suitable for use in the title although the subject name should be distinct enough to identify the information within as some records will contain similar information. Common elements of a title include:

- Date
- Subject
- Version number

8.3 Staff members should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.

## **9. E-mails**

9.1 The email system is a communication tool and is not an appropriate solution for long term file storage. All emails that are records of business activity should be saved to an appropriate folder on the shared network drive in a timely manner.

9.2 Under no circumstances should a member of staff save all emails to the shared drive. This will result in a significant storage burden and information will become difficult to locate. This could result in the OPCC breaching its statutory requirements under FOIA and Data Protection legislation.

9.3 As per Gwent Police policy, unless emails are saved to the shared drive they will automatically be deleted once they are 12 months old.

9.4 Documents which may be attached to an email and need to be saved as a corporate record must be saved separately to the shared drive and not simply retained on an email. This will ensure they are available to all staff who need to access them.

9.5 Unless passed over a secure network, the content of e-mails and attached documents should be regarded as being open to the public. Information which is not suitable for the public domain should not be processed or stored on personal computing equipment.

9.6 Material marked as 'Official-Sensitive' or above should not be sent electronically to personal, unsecure email addresses (with the exception of the Joint Audit Committee agendas) except in exceptional circumstances and with the approval of the Chief Executive.

9.7 No emails should be sent in relation to a work related matter from or to a member of staffs personal email address unless there is a valid reason for doing so. In the case that personal email is used for work related matters, all relevant emails/documentation should be saved on the shared drive once appropriate. Under no circumstance should a personal email addresses be used to store work related information.

9.8 Other forms of electronic communication such as instant messages through the Skype or Microsoft Teams systems will also fall under this policy and will be retained in line with emails unless saved to the shared drive or deleted by the user.

## **10. Inactive Records**

10.1 Responsibility for inactive records (both electronically and in hard copy) will lie with the folder owner as allocated on the retention and disposal schedule and the Information Asset Register.

- 10.2 Any hard copy records stored on desks or in personal drawers/lockers will be the responsibility of the person they belong to.
- 10.3 Inactive records should be subject to review. The record owner should determine if the record needs to be disposed of or retained. If the record needs to be retained then it should be considered for archiving if appropriate.
- 10.4 The HoAC should be advised of any electronic or hard copy records deemed to be suitable for archiving. A review of the information will take place and if appropriate will be archived internally on the Sharepoint system after approval has been sought from the Chief Executive.
- 10.5 Any records deemed to be of historical importance will be archived with Gwent Archives in line with the Retention and Disposal Schedule and Archiving Policy and Procedure. A review of all information will take place on the appointment of a new PCC.

## **11. Accessibility**

- 11.1 It will be the responsibility of the HoAC in conjunction with the Chief Executive to determine which records need to be restricted and who has access to them. Access to confidential electronic records, including personal files, will be restricted to the Chief Executive and HoAC and other identified individuals with a role related need.

## **12. Website**

- 12.1 The Head of Communications and Engagement, with support from other OPCC staff members, will have responsibility for managing the content and updating the OPCC's website. This will include undertaking a review of information stored on the website to ensure compliance with the required legislation.

## **13. Partnership Working and Commissioned Services**

- 13.1 Where records are created as a result of partnership working there needs to be a clearly defined responsibility between the OPCC and the partner organisation/s for the creation, management and deletion of records.
- 13.2 Where the OPCC is the lead partner the relevant OPCC records management policies and procedures be followed, unless agreed otherwise.
- 13.3 Where another organisation is the lead partner the relevant records management policies of the lead organisation are applicable unless agreed otherwise. The OPCC should identify and retain records relating to its role in the partnership as required for its own business. These records should be retained in line with the OPCC's Records Management Policy.



13.4 Where there is no identified lead partner, the OPCC should ensure that provisions are made for one of the partners to assume responsibility for the management of records.

#### **14. Security of Records and Maintenance**

14.1 Records management systems will be designed so that records can be maintained securely, with appropriate safeguards and access controls in place.

14.2 Where staff have to leave their desks in the office unattended they should ensure that their computer is locked and that no sensitive information is left on display but is put away in a secure location.

#### **15. Government Security Classification System**

15.1 Gwent Police uses the Government Security Classification System and every document from them is marked 'Official', 'Official – Sensitive', 'Secret' or 'Top Secret'. The same system will be adopted in respect of the information created, maintained and stored by the OPCC.

15.2 It is the responsibility of the originator to classify the document and control initial circulation which should be limited to those who 'need to know'.

15.3 Records of a sensitive nature must be destroyed using approved methods. 'Official' and 'Official-Sensitive' material can be placed in 'Official-Sensitive' locked waste bins whereas 'Secret' material must be shredded. Further information can be found in the Gwent Police Disposal Policy.

#### **16. Compliance and Review**

16.1 The OPCC undertakes to regularly audit its records management policies to ensure compliance and to incorporate any changes that need to be made.

16.2 Spot checks will be carried out periodically by the HoAC supported by the Governance Officer to ensure compliance with the policies, the outcomes of which will then be reported to the Chief Executive.

16.3 This policy will be reviewed by the HoAC as appropriate but no less frequently than every 4 years.