STANDARD OPERATING PROCEDURES:

OFFICE OF THE BEDFORDSHIRE POLICE AND CRIME COMMISSIONER

Title	Record Management, Retention and Disposal Policy
Area of Compliance	Compliance
Version No.	5.0
Senior Lead	Head of Governance and Transparency
Author	Compliance

Revision History

Date	Revision	Change	Review Date
December 2015	1.0		December 2016
29/09/2017	2.0	Full review completed	29/09/2017
15/05/2018	3.0	Full GDPR review	15/05/2019
15/05/2019	3.0	No Change	15/05/2020
20/09/2020	3.0	No Change	20/09/2021
17/09/2021	3.0	Complaints Policy website link updated	17/09/2022
17/10/2022	4.0	OPCC Logo Updated, update of Protective Marking Scheme	17/09/2023
27/09/2023	5.0	Accessibility amendments, Updated Article 5 wording, updated links	27/09/2024
20/08/2024	5.0	No Change	20/08/2025

Introduction

The Office of Police and Crime Commissioner (OPCC) for Bedfordshire 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 OPCC for Bedfordshire has a responsibility to be accountable to the public for their actions. Therefore, the records must be accurate and capture accurate details. 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 UK General Data Protection Regulations (GDPR) and the Freedom of Information Act 2000 (FOIA).

This policy statement sets out how the OPCC for Bedfordshire 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 deletion of documents.

Under the GDPR the OPCC has a number of responsibilities as both a 'data controller' and 'data processor'. The OPCC will use personal information and may, on occasion, use some categories of sensitive personal information in order to carry out our official functions or public tasks that are set out in law, mainly the Police Reform and Social Responsibility Act 2011. For example, when a complaint is made against the Chief Constable, the Commissioner's Office (OPCC) will retain and process the personal information shared with us in order to carry out the lawful public task of investigating this complaint.

Article 5 of the GDPR requires that personal data shall be:

Personal data shall be:

(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d)accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e)kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(f)processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

Article 5(2) requires that:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

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 lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever any organisation processes personal data:
(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

We may collect personal information to process an enquiry, manage a bid for services or a contract and, subject to consent to partners and members of the public about other events and activities that we think may be of interest to them.

When a complaint is made against the Chief Constable, the OPCC will retain and process the personal information shared with us in order to carry out the lawful public task of investigating this complaint. The OPCC will also respond quickly to share any personal information with Bedfordshire Police when it relates to a risk to life or the need to protect and safeguard the public.

In order to process any complaint or issue of dissatisfaction raised against Bedfordshire Police, its officers and staff, the Commissioner is required to share relevant personal information with Bedfordshire Police Force to ensure that the complaint is looked into and to meet our public task - *(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law*.

The OPCC will pass relevant personal information to Bedfordshire Police Force (including where necessary the parts of Bedfordshire Police Force that are collaborated with Hertfordshire and Cambridgeshire Constabularies) so that they may offer the individual a response to a complaint or issue of dissatisfaction that reflects the operational role of the police force.

More information on how the OPCC process complaints is available within the Complaints policy.

Bedfordshire OPCC will not share personal information with other organisations or companies without a lawful purpose (as set out under Article 6 GDPR 2018) or without the explicit consent of the data subject.

In processing any bid for a contract to provide services, the OPCC may share data with Bedfordshire Police Force, credit reference agencies and fraud prevention agencies, consent to share information will be sought from bidding organisations via the grant application form.

The Freedom of Information Act and Subject Access Requests

Under the Freedom of Information Act and the Environmental Information Regulations the public have a right to request any recorded information held by a public authority.

Any individual has the right to ask for any information that think a public authority may hold. The right only covers recorded information which includes information held

on computers, in emails and in printed or handwritten documents as well as images, video and audio recordings.

They can do this in writing. The public authority must tell the applicant whether it holds the information. A public authority can only refuse to confirm or deny whether it holds the information if this would in itself reveal information that falls under an exemption. The public authority must supply it within 20 working days, in the format requested. The Act applies to all information, not just information held since the Act came into force.

Guidance on how to submit a Freedom of Information request is available via the Information Commissioners Office website.

Guidance on how to submit a subject access request is available via the Information Commissioners Office website.

In some circumstances information may not be provided in response to a data access request because it is exempt, for example because it would unfairly reveal personal details about somebody else. 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.

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 note, 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 and updated 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

Electronic records

Electronic records will be held in structured folders and will logically group information together with security arrangements to ensure that 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, to the designated Data Protection Officer (DPO) for the OPCC, who will follow an agreed Data Breach Management Plan. Any data breach will be recorded, investigated, and reported to the Information Commissioner's Office via the Information Management Unit as appropriate.

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, a report will be submitted in all cases to the Data Protection Officer.

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 ‘Official sensitive’, ‘Restricted’ or ‘Confidential’ should not be sent electronically to personal, unsecure email addresses.

The OPCC electronic system is delivered by the Tri-Force and procedures will reflect the requirements outlined in the Tri-Force Joint Information Management Strategy (IMS).

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

Protective Marking Scheme
Those handling police information have a responsibility to value and safeguard all information they send or receive. Where necessary, appropriate classification and measures should be clearly identified in order to enable sharing and to protect from loss, damage or unauthorised and inappropriate access to the information. Classification ensures that police information is handled appropriately in order to protect individual rights in accordance with the law (part 3, chapter 2, section 40 Data Protection Act 2018) and with respect for the wider public interest.

Although there is no direct correlation between the new Government Security Classification (GSC) and outgoing Government Protective Marking Scheme (GPMS), the below demonstrates how GSC compares with GPMS. It also identifies the three new categories and the use of OFFICIAL-SENSITIVE within OFFICIAL:

Government Protective Marking Scheme (GPMS): Top Secret, Secret, Confidential, Restricted, Protect, NPM

Government Security Classification (GSC): Top Secret, Secret, Official [Official-Sensitive]

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 regularly reviews their Record Management Retention and Disposal Policy, but no less frequently than every twelve months. Records management procedures are in place 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 below Record Retention and Disposal Schedules. 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 either the Freedom of Information Act or Data Protection 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;
- 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.

Record Retention and Disposal Schedules

Contents

1 OFFICE OF THE POLICE AND CRIME COMMISSIONER

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
1.1	Appointment of Chief Constable	Advertisements, Application Forms, Interview Reports. Personnel Files	2 years 6 years from date of last pension payment	Common Practice Common Practice	E-copy – delete Hardcopy – Confidential shred
1.2	Audit Committee meetings	Minutes, agendas, reports, indexes Draft and audio minutes Background papers Terms of reference Membership	Permanent Destroy once minutes are formally approved 4 years from date of production at meeting Until superseded	Common Practice Common Practice Common Practice Common Practice	Archive E-copy – delete Hardcopy – Confidential shred
1.3	Complaints against the Chief Constable	Correspondence	6 Years after finalisation	Common Practice	E-copy – delete Hardcopy – Confidential shred
1.4	Complaints and enquiries directed to the OPCC	Correspondence, summary reports, details of investigations	6 Years after finalisation	Common Practice	E-copy – delete Hardcopy – Confidential shred
1.5	Corporate planning and reporting	Police and Crime Plans Strategic Plans Annual Reports	Permanent	Common Practice	Archive
1.6	Dismissal of the Chief Constable	Resignation, redundancy, dismissal, death, retirement	6 years after termination or, if pension paid, 6 years after last pension payment	Common Practice	E-copy – delete Hardcopy – Confidential shred

1.7	Employment Tribunals	Cases	6 years after last action	Common Practice	E-copy – delete Hardcopy – Confidential shred

1.8	External Meetings (where the OPCC does not own the record)	Minutes, agendas and reports	3 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
1.9	Independent Custody Visiting Scheme	Panel minutes, agendas, reports Visiting reports, rotas, Panel contact details Personnel files Scheme/handbook Complaints against Visitors Newsletters Expense Claims	2 years 6 years Until age 100. Consider age 85 years of age for non-pay/pension records Until superseded On termination of membership 2 years 6 years from termination of membership	Common Practice Common Practice Common Practice Common Practice Common Practice Common Practice Common Practice	E-copy – delete Hardcopy – Confidential shred
1.10	Independent Members serving on Police Misconduct Panels and Audit Committees	Personnel files Expense Claims Scheme/handbook Complaints against Independent members	Until age 100. Consider age 85 years of age for non-pay/pension records 6 years from termination of membership Until superseded Permanent	Common Practice Common Practice Common Practice Common Practice	Archive E-copy – delete Hardcopy – Confidential shred Archive
1.11	Partnership, agency and other meetings (where the OPCC owns the record)	Minutes, agendas and reports	Permanent	Common Practice	Archive
1.12	Police Appeal Tribunals	Cases	Permanent	Common Practice	Archive
1.13	Statutory Inspections, reviews and external audit reports	Reports	Permanent	Common Practice	Archive

1.14	Statutory returns	Reports to Central Government	7 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
1.15	Working Groups / Project Boards	Minutes, agendas and reports	5 years	Common Practice	E-copy – delete Hardcopy – Confidential shred

2 POLICE AND CRIME COMMISSIONERS /DEPUTY POLICE AND CRIME COMMISSIONERS

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
2.1	Appointment	Personnel Files Advertisements, application forms, interview notes Legislation/national guidance	Until age 100. Consider age 85 years of age for non-pay/pension records 2 years after date of appointment until superseded	Common Practice Common Practice Common Practice	Archive E-copy – delete Hardcopy – Confidential shred
2.2	Conduct	Complaint Cases	Permanent	Common Practice	Archive Scan into E-copy
2.3	Payments	Salary and allowances	6 years from termination of membership	Common Practice	E-copy – delete Hardcopy – Confidential shred
2.4	Registers of Interests, Gifts and Hospitality	Register of Interests Register of Gifts and Hospitality	Permanent	Common Practice	Archive – E-copy must be kept

3 MANAGEMENT AND ADMINISTRATION

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
3.1	Association of Police and Crime Commissioners (APCC) Circulars	Circulars	Permanent	Common Practice	Archive – E-Copy
3.2	Diaries and calendars	Electronic and manual diaries and calendars	3 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
3.3	Enquiries – Other OPCCs and general	Routine responses to enquires	1 year	Common Practice	E-copy – delete Hardcopy – Confidential shred
3.4	General correspondence	Correspondence – minor and routine	1 year	Common Practice	E-copy – delete Hardcopy – Confidential shred
3.5	Home Office Circulars	Circulars	1 year	Common Practice	Archive – E-Copy

3.6	Information Management	Filing indices	Permanent	Common Practice	Archive
		Records of transfers to archives	12 years	Common Practice	E-copy – delete Hardcopy –
		Summary of responses to enquiries Disposal records Reports/correspondence on OPCC action	6 years	Common Practice	Confidential shred
		Routine responses to enquiries	2 years	Common Practice	E-copy – delete Hardcopy –
		General Correspondence/emails and faxes	Archive for 1 year – destroy if no further use. No file should remain open for more than 5 years and may be closed at any time within	5 year rule specified in Code of Practice on Records	Confidential shred

			the period based on monitoring of usage and additions. If closed and new activity begins, a new volume of the file should be created, and the retention period of the old volume be brought in line with the new volume.	Management under s46 Freedom of Information Act 2000.	
3.7	Marketing	Developing and promoting OPCC events Information about the OPCC	2 years When superseded	Common Practice Common Practice	E-copy – delete Hardcopy – Confidential shred
3.8	Media Relations	Media reports Media releases	3 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
3.9	Newsletter	OPCC Newsletter	1 year	Common Practice	E-copy – delete Hardcopy – Confidential shred

3.10	Office Management	Contracts with suppliers	12 years if sealed 7 years from end of contract	Common Practice	E-copy – delete Hardcopy – Confidential shred
3.11	Policy Development	Policies Instructions/Rules/Procedures Organisational Charts Financial and Contract Regulations Routine responses on policy or procedures (printed material, letters)	25 years then review and archive 1 year after revision	Common Practice Common Practice	Archive E-copy – delete Hardcopy – Confidential shred
3.12	Policy/strategy review	Reports and supporting documentation	5 years from closure		E-copy – delete Hardcopy – Confidential shred
3.13	Publications	The process of designing and setting information for publication The published work of the OPCC	3 years from the last action Destroy after administrative use is concluded. Note one copy from the initial print run should go directly to the archive.	Common Practice Common Practice	E-copy – delete Hardcopy – Confidential shred
3.14	Public Consultation	Consultation on development of significant policies Consultation on development of minor policies Consultation meeting notes, records, correspondence, minutes, supporting papers and correspondence	5 years 1 year 2 years	Common Practice Common Practice Common Practice	E-copy – delete Hardcopy – Confidential shred

3.15	Quality and Performance	OPCC Inspection/ Best Value Review reports	5 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
3.16	Unstructured records	Records that do not support a business process i.e. there is not an existing place for them in a filing structure and none will be created. This applies to filing structures for paper and electronic formats including e-mails. Working papers which lead to a final report (unless report is submitted to Committee – in which case papers should be available for 6 years in line with availability of the minutes for public inspection)	Destroy as soon as use has ceased	Local Government Act 1972 – Access to information for working papers as background to reports to Committee	E-copy – delete Hardcopy – Confidential shred

4 LEGAL AND CONTRACTS

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
4.1	Agreements	Service level agreements with the OPCC	6 years after agreement expires	Common Practice. Depends on value of agreement. Mainly to do with agreements between public bodies. Not in regard to contracts.	E-copy – delete Hardcopy – Confidential shred
4.2	Asset acquisition/disposal	Legal docs relating to purchase/sale Leases Tender documents	3 years	Common Practice Common Practice	E-copy – delete Hardcopy – CONFIDENTIAL SHRED
4.3	Contract development (ordinary)	Tender specification	6 years after terms have expired	Statutory	E-copy – delete Hardcopy – Confidential shred
4.4	Contract development (under seal)	Tender specification	12 years after terms have expired	Statutory	E-copy – delete Hardcopy – Confidential shred
4.5	Conveyance	Conveyance files	12 years after closure.	Statutory	E-copy – delete Hardcopy – Confidential shred
4.6	Evaluation of tenders (ordinary)	Evaluation criteria Successful tender document	6 years after terms have expired	Statutory	E-copy – delete Hardcopy – Confidential shred

4.7	Legal Advice	Correspondence Fees	3 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
4.8	Litigation	Correspondence Criminal and civil case files	7 years after last action	Common Practice	E-copy – delete Hardcopy – Confidential shred
4.9	Post tender negotiation	Minutes Correspondence	1 year after terms of contract have expired	Common Practice	E-copy – delete Hardcopy – Confidential shred
4.10	Tenders	Tender envelope	1 year after start of contract	Statutory	E-copy – delete Hardcopy – Confidential shred
4.11	Unsuccessful tender documents	Tender documents quotations	1 year after start of contract.	Common Practice	E-copy – delete Hardcopy – Confidential shred

5 HUMAN RESOURCES

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
5.1	Appointment of Statutory Officers	Vacancies and applications records Interview notes prospective staff Records Registers of applicants Unsuccessful application records	2 years after date of appointment	Common Practice	E-copy – delete Hardcopy – Confidential shred
5.2	Disciplinary and Grievance investigations (proved)	Disciplinary records Grievance records	Oral warning – 6 months Written warning – 1 year Final warning – 18 months Dismissal – after determination of all internal and external appeals – 2years	Common Practice	E-copy – delete Hardcopy – Confidential shred
5.3	Disciplinary and Grievance investigations (unproved)	Disciplinary records Grievance records	3 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
5.4	Employee relations	Agreements Correspondence re Formal negotiations Correspondence re minor and routine matters	Permanent 2 years	Common Practice	Archive E-copy – delete Hardcopy – Confidential shred
5.5	Equal Employment Opportunities	The process of investigation and reporting on specific cases to ensure that entitlements and obligations are in accordance with agreed Equal Employment Opportunities guidelines policies.	5 years after action completed	Common Practice	E-copy – delete Hardcopy – Confidential shred
5.6	Medical Records	Medical examinations Adjustment to work examinations	72 years after DOB	Common Practice	E-copy – delete Hardcopy – Confidential shred
5.7	PDR	Probation reports Performance reports and plans	5 years after action completed	Common Practice	E-copy – delete Hardcopy – Confidential shred

5.8	Personnel administration	Establishment lists Personnel files	Permanent Destroy 6 years from date of last pension payment/leaving date	Common Practice	Archive E-copy – delete Hardcopy – Confidential shred
5.9	Recruitment – the selection and appointment of an individual for an established position	Advertisement, application forms, references, interview reports Vetting checks and associated documentation	1 year after appointment made. Positive outcomes – 2 years after date of check. Negative outcomes – 1 year after date of check.	Common Practice Common Practice	E-copy – delete Hardcopy – Confidential shred
5.10	Staff leave/Sickness monitoring	Sickness records Leave records Flexi cards	Until age 72	Common Practice	E-copy – delete Hardcopy – Confidential shred
5.11	Staff retention	Financial reward	Destroy 7 years after action completed	All records relating to actual payments are dealt with under Finance	E-copy – delete Hardcopy – Confidential shred
5.12	Staff termination	Resignation, redundancy, dismissal, death or retirement	6 years after termination or, if pension paid, 6 years after last pension payment	Common Practice	E-copy – delete Hardcopy – Confidential shred

6 FINANCIAL MANAGEMENT

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
6.1	Annual reports	Annual Statement of Accounts	Permanent	Common Practice	Archive
6.2	Approvals/process for purchase	Purchase/sales order	7 years after end of financial year	Statutory	E-copy – delete Hardcopy – Confidential shred
6.3	Asset Acquisition and Disposal	Management of the acquisition (by financial lease of purchase) and disposal (by sale or write off) process for assets	6 years, if under £50,000 or 12 years if over £50,000, after all obligations / entitlements are concluded	Statutory	E-copy – delete Hardcopy – Confidential shred
6.4	Asset monitoring and maintenance	Asset registers Inventories Stocktaking Acquisition & disposal reports Service/maintenance records	7 years after the end of the financial year 2 years after admin use 7 years after sale or disposal	Statutory Common Practice Statutory	E-copy – delete Hardcopy – Confidential shred
6.5	Budget setting	Final annual budget Draft budgets and estimates Quarterly budget reviews	Permanent 2 years after budget set Destroy after following years budget adopted	Only final version of annual budget needs to be kept Common Practice Common Practice	Archive E-copy – delete Hardcopy – Confidential shred

6.6	Expenditure	Invoices/receipts Bank statements Vouchers/ledger Write offs of public monies Processes to balance and reconcile financial accounts	6 years after end of financial year 2 years after admin use is concluded	Statutory Common Practice	E-copy – delete Hardcopy – Confidential shred E-copy – delete Hardcopy – Confidential shred
6.7	Finance reports	Quarterly budget reports Working papers	Destroy when admin use complete	Common Practice	E-copy – delete Hardcopy – Confidential shred
6.8	Internal Audit	Internal Audit reports – main financial and subsidiary systems Value for money studies Working papers Follow up audits	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	Common Practice Common Practice	E-copy – delete Hardcopy – Confidential shred
6.9	Loans	Loan files (borrowing money to enable authority to perform its functions and exercise its powers) Loans register/summary management of loans	Destroy after the loan has been repaid Permanent	Statutory Common Practice	E-copy – delete Hardcopy – Confidential shred Archive
6.10	Payroll	Claim forms Pay/tax records Summary pay reports Non accountable processes relating to payment of employees	7 years after the end of the financial year Destroy after admin use	Statutory Common Practice	E-copy –delete Hardcopy – Confidential shred

7 PROPERTY AND LAND MANAGEMENT

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
7.1	Insurance	Insurance policies Correspondence	7 years after terms expire	Common Practice	E-copy – delete Hardcopy – Confidential shred
7.2	Management of buildings of special interest	Project specification Plans Certificates of approval	Permanent	Common Practice	Archive
7.3	Property acquisition	Plans	Life of property plus 12 years	Common Practice	E-copy – delete Hardcopy – Confidential shred
7.4	Property disposal	Legal documents Survey reports Tender documents Conditions of contracts	15 years after all obligations end	Common Practice	E-copy – delete Hardcopy – Confidential shred
7.5	Property inventories	Inventories	Permanent	Common Practice	Archive

8 GENERAL

	Function	Records	Retention	Statutory Provisions/Authority	Method of disposal
8.1	Freedom of Information requests where exemptions apply, complaints or appeals are made	Requests for information dealt with under the provisions of the Freedom of Information Act 2000 where: The records are subject to exemptions (partially or wholly), A Public Interest Test has been formally applied, A complaint has been made to OPCC about the application of exemptions or handling of the request, A complaint has been made to the Information Commissioner about the application of exemptions or the handling of the request	The request itself, associated records, and any records to which the request applies should not be destroyed until LPA is satisfied that requestor does not wish to pursue an appeal or the appeal process has been exhausted. The documentation should remain current for 1 year from the last action, then closed for 1 further year, then destroyed if no further activity has occurred. Should an activity occur within that period, the documentation should become current again.	Freedom of Information request (not routine); Correspondence with requestor/Information Commissioner; Correspondence in locating records; Records of public interest tests and exemptions decisions; Details of records relating to the request (references, titles, locations, owners).	E-copy – delete Hardcopy – Confidential shred
8.2	Health and Safety	Risk assessments Accident books/RIDDOR correspondence and fire certificates	Risk Assessments current plus 10 years, Accident books 3 years from last entry and Fire certificates until superseded	Common Practice	E-copy – delete Hardcopy – Confidential shred