Records Destruction Procedures

Information Governance and Records Management Policy

Procedures relating to:	Information Governance and Records Management Policy
Consultation via:	Global Information Governance and Data Protection Committee
Effective date:	1 August 2024
Review period:	Five years from effective date, or more frequently if required
Responsible Executive	Secretary of the University
Responsible Office:	Information Governance division

HERIOT-WATT UNIVERSITY
RECORDS DESTRUCTION PROCEDURES

CONTENT

1. INTRODUCTION

1.1 The Information Governance and Records Management Policy ('the Policy') sets out the information governance principles the University applies to be accountable for, and transparent about, its activities. This Procedure (the Records Destruction Procedure) supports the implementation of the information governance principle:

> *We create, receive, and maintain information assets that have a defined Lifecycle*

1.2 Different types of information have lifecycles of differing length. Retaining information we no longer need is a waste of finite resources and presents compliance risks. For example, information consumes:

- Staff time and attention in maintaining and searching through it to find the 'right information'
- Physical storage space. Off-site storage has a financial cost. On-site storage also has an opportunity cost.
- Server space. Digital storage has both a financial cost and an environmental cost as vast quantities of electricity are required to maintain and cool large server farms.

Moreover, under data protection laws we can be subject to regulatory investigation, sued or fined up to £500,000 for breaches that cause damage to data subjects. Retaining information longer than necessary is a data protection breach and can be compounded if the information is also subject to an information security breach.

1.3 The University's retention schedules set out how long it is necessary to retain information. They set out the lifecycles for university records that are the 'lead copy', sometimes also known as the 'master copy', 'golden copy' or 'single point of truth'. Our retention schedules help to ensure that we retain information for as long as it is needed for business, legal or regulatory purposes, but no longer. This is necessary to comply with legislation, regulations, audit requirements and good practice. Some lifecycles are relatively short (e.g. one year) while others may be much longer (40 years or more). Sections 3 and 4 of this Procedure set out how to dispose of records in accordance with our retention schedules.

1.4 Copies of records which are not the 'lead copy' are 'reference copies'. Reference copies are 'transitory information'. University retention schedules do not apply to 'transitory information'. Transitory information has only temporary value. It has no significant informational or evidential value after it has served its primary purpose. It can usually be disposed of within no more than 6 months, or in the case of 'reference copies', as soon as they are no longer needed for reference. Transitory information is produced:

- In the completion of routine actions (ephemeral records)
- In the preparation of other records which supersede them (temporary records)
- for convenience of reference (reference copies)

Section 2 of this Procedure sets out how to dispose of 'transitory information'.

1.5 Once information reaches the end of its defined lifecycle it must be disposed of appropriately. This is known as 'disposition'. The University has two disposition actions:

- securely and permanently destroy, or
- transfer to the University Museum and Archive for permanent preservation for future generations

This Procedure provides step by step instructions for securely and permanently destroying information. Instructions for transferring information to the University Museum and Archive are provided in the Archive Transfer Procedures [to follow].

1.7 This Procedure, like the Policy, applies to all information assets created, received, and maintained in the course of university business by anyone working on behalf of the University, in all formats, of any age, wherever they are created, used, stored, or held. Information assets include data (and personal data), information, and records. For example this procedure applies to traditional paper files, emails, instant messages, digital documents on SharePoint, Teams, and traditional network drives, etc.

1.8 This Procedure provides step by step instructions for:

- Everyone working on behalf of the University to apply good housekeeping principles to routinely and regularly dispose of transitory information (see section 2 below), and
- Local Information Asset Managers (LIAMs) to lead their business units in implementing the University's retention schedules (see section 3 below).
- Heritage and Information Governance teams to appraise and dispose of records held in the legacy records management service (see section 4 below)

1.9 Some words and phrases in this Procedure have specific definitions that are provided in section 7 below. For example: Archival value; disposition; disposition action; disposition authority; disposition hold; disposition records; information security classification scheme; records; record series; retention schedule; transitory information.

2. PROCEDURE FOR DISPOSING OF TRANSITORY INFORMATION

2.1 Under section 5.1 of the Policy, everyone working on behalf of the University is responsible for applying good housekeeping principles by routinely and regularly disposing of transitory information as soon as it reaches the end of its lifecycle and is no longer required.

2.2 The method used to dispose of transitory information will depend on its format and content. Appendix 1 provides a destruction methods matrix to help you to identify the appropriate method.

2.3 The destruction of transitory information is the responsibility of individual users and **does not** require 'disposition records' such as a Destruction Log (appendix 2) or authorisation.

Examples of transitory information which can be routinely destroyed:

2.4 Duplicates which are produced **for reference only** and which are exact copies of originals kept in a recordkeeping system. E.g. Photocopies of paper documents; electronic or printed copies of electronic documents; duplicate copies of photographs, audio or video recordings; reference sets of meeting papers, technical reports, plans etc.

2.5 Draft documents and working materials which do not document significant steps in the development of a final version, and which are not needed to track the development process or provide evidence of decisions or precedents. E.g. draft documents with only proofreading marks; initial outlines of ideas, designs, calculations etc. which were discarded or incorporated into other work which superseded them; unused audio/video material which was discarded during editing; unofficial work planning or scheduling materials or communications.

2.6 Documents containing requests for information which have no further value after the information is provided/received. E.g. requests for 'stock' publications, maps/directions, arrangements for events.

2.7 Transmittal documents which accompany records, but which do not themselves contain substantive information and are not required as evidence of receipt. E.g. fax cover sheets/header slips, compliments slips, sticky notes, routing slips etc. (paper or electronic) which contain only transmittal information (names, contact details etc.)

2.8 Items **received for information only** from elsewhere in the institution, often as part of a distribution list. E.g. 'All Staff' emails and notices; publications for staff (e.g. NewsBeat); publications for general distribution (e.g. prospectuses, plans, marketing materials). N.B. The business unit which produced these items must retain the official records and manage them in accordance with the Information Governance and Records Management Policy.

2.9 Items received (solicited or unsolicited) **for information only** from external organisations. E.g. advertising materials (e.g. brochures, catalogues, price lists), email messages received from listservs, publications (e.g. magazines, newsletters, etc.).

3. PROCEDURE FOR DISPOSING OF UNIVERSITY RECORDS HELD BY SCHOOLS AND PROFESSIONAL SERVICES

3.1 Under section 5.1 of the Policy, everyone working on behalf of the University is responsible for working with their manager, local Information Asset Manager (LIAM) and colleagues to apply the University's records retention schedules.

3.2 The relevant LIAM (or head of unit) must supervise the process described in section 3 of this Procedure, but they may delegate individual steps as necessary.

3.3 Each business unit will conduct dispositions at least once a year as part of their regular information management routine. LIAMs will determine the most appropriate time(s) of year for their business unit to carry out this process. In many cases the start or end of the academic, financial or calendar year are suitable.

Step 1: Identify records due for destruction

3.4 LIAMs (or their delegate) will identify records due for destruction. Records are due for manual destruction under this procedure when they:

- are closed
- have completed the retention period stated in the retention schedule
- have a disposition action of 'destroy', and
- are not covered by an automated deletion policy (e.g. M365 retention label)

If the disposition action is 'transfer to archive', do not destroy the records, instead refer to the Archive Transfer Procedures [to follow].

3.5 LIAMs understand the records for which they are responsible. Records covered by this procedure include:

- Paper records held on campus and in off-campus locations such as the Records Storage and Retrieval Service (RSRS)
- Digital records on network drives
- Digital records on OneDrive, SharePoint, and Teams (not covered by an automated deletion or retention policy)
- Emails held in generic accounts and individual user accounts (not covered by an automated deletion or retention policy)
- Records held in line of business applications (not covered by an automated deletion or retention policy)

LIAMs will use their knowledge of the records held by their unit and refer to the published retention schedules to identify the retention periods for those records. Advice on using the retention schedules is available on the Information Governance Intranet and by contacting InfoGov@hw.ac.uk.

Step 2: List records due for destruction

3.6 LIAMs (or their delegate) will keep 'disposition records' to provide an audit trail to demonstrate that destroyed records were legitimately destroyed in accordance with the University's policy and procedures. This is an important stage and must not be omitted. Keeping disposition records will, for example, help to defend against any allegations under section 65 of the Freedom of Information (Scotland) Act 2002 which makes it a personal criminal offence to destroy information which is the subject of an information request.

3.7 LIAMs (or their delegate) are encouraged to use the Destruction Log in Appendix 2 to create a list of the records due for destruction. If not using the Destruction Log, LIAMs must keep equivalent records containing similar information. LIAMs can download a Destruction Log template from the Information Governance Intranet.

3.8 If using the Log, LIAMs (or their delegate) will add the name of their business unit, and their name as the 'compiler' of the Log. The compiler will add descriptions of the records to be destroyed, grouped by 'records series'. Do not list individual documents, files, or folders. At this stage provide:

- Records series title
- Long description
- Covering dates
- Disposition authority reference (i.e. the retention schedule or retention period being applied)

Appendix 2 provides some example entries giving an indication of the level of detail required. Some Logs may only contain a very few rows.

Step 3: Check whether any 'disposition holds' are in place

3.9 The compiler will check whether any 'disposition holds' are in place. A 'disposition hold' puts a temporary halt on the disposition of records which are required for legal or regulatory purposes. Once the legal or regulatory issue has been resolved, the 'hold' is lifted, and the disposition can resume.

3.10 Records containing information which has been requested under freedom of information or data protection laws must not be destroyed until the request has been fully resolved and the appeal period has expired. Contact FOI@hw.ac.uk if you are unsure whether this applies to any of the records on your destruction log.

3.11 Records that may be required as part of an ongoing legal action must not be destroyed until the legal action is fully resolved. Contact Legal Services (if you are unsure whether this applies to any of the records on your destruction log.

3.12 If using the destruction log template, the compiler will create a new row for any records to which a disposition hold applies and add 'Disposition Hold' in the destruction method column for the row. Appendix 2 provides an example.

Step 4: Authorise destruction

3.13 Destructions must not be carried out until they have been authorised. Destructions must be authorised in writing by the relevant Information Asset Owner (IAO) or their nominee.

3.14 The IAO (or their nominee) must review the destruction log (or equivalent documentation) and satisfy themselves that the records described can be destroyed and that any disposition holds have been applied correctly. This may involve seeking advice from the Information Governance division.

3.15 The IAO may be aware of emerging legal or regulatory issues that mean the destruction of some of the records should be delayed. Where this is the case, it must be documented on the destruction log (or equivalent) and in accompanying disposition records.

3.16 When the IAO is ready to approve the destructions, they must complete the 'Authorisation' section of the log by signing and dating it before returning it to the compiler.

Step 5: Carry out destructions

3.17 Once authorisation has been received, the compiler will contact the staff with day-to-day responsibility for the records and instruct them to carry out the destructions.

3.18 Staff must select the most appropriate destruction method according to the format and content of the records by referring to the matrix and guidance in Appendix 1. Staff must never retain copies of destroyed records.

3.19 Staff must update the destruction log (or equivalent) with:

- The destruction method used
- Their name
- The date destruction occurred

Step 6: Record-keeping

3.20 The compiler will complete the destruction log (or equivalent) with any further relevant notes and attach relevant accompanying documentation such as:

- Correspondence detailing any disposition holds or the absence of disposition holds
- Correspondence with the IAO and/or the colleague who authorised the destructions
- Any destruction certificates provided by third party contractors

3.21 The compiler will send the completed destruction log (or equivalent) and accompanying documentation to InfoGov@hw.a.uk, cc'd to the colleague who authorised the destructions. The Information Governance division will retain this documentation for 25 years, as evidence of compliance with HWU retention schedules and the legal obligations they represent.

4. PROCEDURE FOR REVIEWING AND DISPOSING OF RECORDS HELD IN THE LEGACY RECORDS MANAGEMENT SERVICE

4.1 Until 2018, the RSRS was provided in-house by the Heritage and Information Governance (HIG) team.

4.2 If appropriate, the Information Governance division will transfer boxes in the legacy service to the appropriate school or professional service account and destructions will be handled as described in section 3 of this procedure. In all other cases, the Information Governance division will follow the procedure outlined below.

Background

4.3 Until 2018, HIG accepted records transfers from business units which were accompanied by a 'transfer sheet' describing the records. When HIG received a transfer they:

- Added information from the transfer sheet onto the records management database
- Assigned a location to the box and the files in the box

- Set a 'review date' for each set of records based on the retention schedule
- Sent a 'confirmation of records transferred memo' to the business unit detailing receipt, location, and review date.

4.4 When review dates came up, HIG sent a report to the business unit's representative, listing those records due for review, with recommendations for their destruction, archiving or retention for a further fixed period. Business units had four weeks from the date of the report to respond, after which time it was assumed that they were in agreement with the recommendations, and HIG actioned the dispositions.

Procedure for review and disposition

4.5 The Information Governance (IG) division will use the existing finding aids to identify:

- Boxes with expiry or review dates that have passed
- Boxes whose descriptions indicate that their contents are due for disposition

4.6 Where the finding aids provide sufficient detail, IG will make a disposition recommendation without reviewing the contents. Where the finding aids do not provide sufficient detail and/or the box does not have an expiry or review date, IG will recall the box, review the contents, and make a disposition recommendation.

4.7 In all cases, IG will:

- Complete a destruction log (appendix 2)
- Make disposition recommendations based on the retention schedules and a consideration of archival value
- Check for any disposition holds

4.8 Where necessary to make disposition recommendations, IG may liaise with others. For example, with the LIAMs responsible for allied records series to confirm whether records are duplicates of those held elsewhere.

4.9 IG will send the destruction log to the IAO, cc'd to the University Archivist, and explain that the records will be destroyed in 4 weeks' time unless they raise an objection.

4.10 IG will respond to any objections raised by the IAO or University Archivist and amend the destruction log accordingly.

4.15 IG will arrange for destruction of the records detailed on the destruction log and retain appropriate disposition records documenting the destructions. The retention period for records documenting the disposal of redundant records is 25 years from the disposal date.

5. RELATED POLICIES AND PROCEDURES AND FURTHER REFERENCES

5.1 This procedure should be read in conjunction with:

- Information Governance and Records Management Policy
- Retention schedules
- Archive Transfer Procedures [to follow]
- The Data Safety Code: Information security classification scheme

6. FURTHER HELP AND ADVICE

For further information and advice about this procedure contact

6.1 Anne Grzybowski
Records Manager
Information Governance Division
Governance and Legal Services
Email: InfoGov@hw.ac.uk

7. DEFINITIONS

Archival value

Long-term research value for cultural purposes. Probably less than five per cent of university records have archival value and need to be preserved permanently in the Heriot-Watt University Museum and Archive. University records with archival value are those which reflect and provide the essential evidence of the University's most significant functions and activities, and also serve legitimate research needs of the University and wider academic and public user community. University records with archival value collectively show how the University was organised and operated, its effect on the wider community and what it did and why.

Disposition

Processes associated with implementing records retention, destruction or archival transfer decisions which are documented in retention schedules.

Disposition action

What happens to a record at the end of its retention period. The disposition action for records that have archival value is 'transfer to archive'. The disposition action for all other records is 'destroy'.

Disposition authority

The instrument that defines the disposition actions that are authorised for specified records. For the University our disposition authorities are the retention schedules approved by the Global Information Governance and Data Protection Committee.

Disposition hold

Applied to records that are due for disposition but need to be retained longer for legal reasons. Disposition holds should be authorised by the Information Asset Owner (or their nominee), normally on the advice of the Head of Information Governance and Data Protection Officer.

For example, the records are the subject of a freedom of information request which is within the review or appeal period, or the records are needed for litigation purposes.

Disposition records

Set out:

- Description of the records (at folder, record series or system level) that have been disposed of
- Method of disposal
- Date of disposal
- Who authorised disposal
- Who carried out disposal (and if carried out by an external contractor, a copy of the destruction certificate)

Information security classification scheme

The University's "Red Amber Green Data Safety Code" which identifies confidential information based on the level of harm that would result if the information were lost, stolen, or accidentally disclosed to others. The scheme provides examples of the main kinds of information used by the University in each category and gives practical advice on what to do to store the information, communicate the information and securely destroy the information when no longer needed.

Record

Recorded information or data (in any format) created, received, or maintained by the University (or someone working or acting on its behalf) in the transaction of university business or conduct of university affairs and kept as evidence of those activities for business, regulatory, legal or accountability purposes.

'Business purposes' are any purposes which support the University's functions and activities. 'Regulatory purposes' are any purposes which support or demonstrate the University's compliance with regulatory requirements. 'Legal purposes' are any purposes which support or demonstrate the University's compliance with any legal obligation. 'Accountability purposes' are any purposes whereby the University answers for its conduct.

Record series

Records maintained as a unit because they result from the same process or activity; have a particular form; or because of some other relationship arising out of their creation, receipt, or use. Examples include: Complaint case files; committee meeting files; student files; academic appeal case files; information request case files

Records Storage & Retrieval Service (RSRS)

The Records Storage & Retrieval Services (RSRS) provides secure off-site storage for physical semi-current records. The service is provided under contract by a third-party supplier. The contract is managed by the Information Governance division.

Most schools and professional services have an account and at least one 'authorised user'. Authorised users are responsible for monitoring the expiry dates of boxes in their account and requesting the timely disposition of boxes that have reached their expiry date, in accordance with section 3 of this Procedure.

Retention schedule

Sets out the agreed length of time the University needs to keep different types of records. Retention schedules are policy documents which support compliance with legislative and regulatory requirements.

Transitory information

Has only temporary value. It is produced:

- In the completion of routine actions (ephemeral records)
- In the preparation of other records which supersede them (temporary records)
- For convenience of reference (reference copies)

Transitory information has no significant informational or evidential value after it has served its primary purpose. It can usually be disposed of within no more than 6 months.

8. PROCEDURE VERSION AND HISTORY

Version No	Date of Approval	Brief Description of Amendment
1	9 May 2024	Presented to the Global Information Governance and Data Protection Committee

APPENDIX 1: DESTRUCTION METHODS

Use the matrix in Table 1 to identify the appropriate destruction method for the information needing to be destroyed.

Keep copies of any destruction certificates with your destruction log (or equivalent).

Table 1: Destruction methods matrix

	Information Security Classification[1]		
	High Risk (Red)	Medium Risk (Amber)	Low Risk (Green)
Digital records	Delete and empty the 'recycle bin' or 'deleted items' folder		
Papers held in offices	Confidential Disposal[2]		Recycling
Removable digital storage media, e.g. floppy discs, CDs, DVDs, USB drives			Waste Management Services[2]
Managed devices, e.g. University issued PCs, laptops, tablets, and mobile phones	Return to Information Services[3]		
Self-managed devices[4]			
BYOD	Permanently erase the data[5]		N/A
Boxes held in the Records Storage & Retrieval Service[6]	Confidential Disposal		N/A

[1] Use the Data Safety Code: Information Security Classification to identify the classification (Red, Amber or Green) of the information due for destruction. If some of the information is green and some is amber or red and applying different methods is impractical, use the destruction method for red and amber information.

[2] Refer to the Procurement Services Intranet pages for help accessing confidential disposal and waste management services.

[3] Always return university owned devices to Information Services (IS). Never pass university owned devices directly to another colleague for use, always return them to IS so that they can be cleansed and reissued.

[4] Self-managed devices are university issued or owned devices that are not fully managed by IS. Self-managed devices must comply with the conditions described at on the IS Intranet pages: Self-managed device guidance.

[5] BYOD (or 'bring your own device') is when personal devices are used to store university information. For example, when you use your personal mobile phone or laptop to download university emails and Teams messages. Never pass equipment that has been used to store or process red or amber category information to other individuals or organisation without first following NCSC guidance and permanently erasing the data. Consider donating your old

equipment through the Tech Donation Box initiative. Visit Information Security Intranet pages for the latest information security guidance on using BYOD.

[6] Refer to the Information Governance Intranet pages for help using the off-site Records Storage & Retrieval Service, including confidential disposal arrangements for boxes held off-site.

APPENDIX 2: RECORDS DESTRUCTION LOG

Business unit: *[Name of your business unit]*

Compiled by: *[Your name, as the person compiling the log]*

Authorisation

Destruction authorised by: *[Name of the person authorising the records to be destroyed]*

Authorisation signature: *[This may be a digital signature]*

Date authorised: *[Date authorisation was given]*

Authorisation comments: *[if any]*

Compiler's Notes *[Use this space to record any further relevant information]*

Description of the records to be destroyed			Disposition authority reference	Description of destruction		
Record series title	Long description	Covering dates		Destruction method	Carried out by	Destruction date
EXAMPLES: *PDR documentation*	*Performance & Development Review (PDR) forms for Institute of Magic staff*	*2019-20*	*RRS for HR (17/06/2015)*	*Confidential waste*	*Hermione Granger*	*01/09/2023*
Student correspondence files	*Routine correspondence with individual Institute of Magic students on issues relating to attendance, progress, health and wellbeing. Graduating year: 2017*	*Aug 2011 to July 2017*	*Student Lifecycle RRS (19/04/2018)*	*Delete*	*Nevill Longbottom*	*31/08/2023*

Description of the records to be destroyed				Description of destruction		
Record series title	Long description	Covering dates	Disposition authority reference	Destruction method	Carried out by	Destruction date
Student complaint files	*Complaint handling case files*	*2016-17*	*Student Lifecycle RRS (19/04/2018)*	*Delete*	*Padma Patil*	*29/08/2023*
Student complaint files	*Complaint handling case file relating to the complaint raise by Theodore Nott. The case is part of an ongoing dispute.*	*June-July 2017*	*N/A*	*DISPOSITION HOLD*	*N/A*	*N/A*

Instructions: Step-by-step instructions for completing this log are provided in the Records Destruction Procedures.

This log is available to download as an Excel spreadsheet from the Information Governance Intranet.

Send the completed Log and copies of any relevant supporting documentation (e.g. correspondence detailing any disposition holds or the absence of disposition holds, correspondence with the IAO and any destruction certificates provided by third party contractors) to InfoGov@hw.ac.uk. The Information Governance division will retain this documentation as evidence of compliance with our retention schedules and the legal obligations they represent for 25 years.