Student records management policy

December 2013

Approving authority:	Secretary's Board,
Consultation via:	Learning and Teaching Administrators' Forum
Approval date:	3 December 2013
Effective date:	3 December 2013
Review period:	Three years from date of approval
Responsible Executive:	Secretary of the University
Responsible Office:	Academic Registry and Heritage and Information Governance

HERIOT-WATT UNIVERSITY

STUDENT RECORDS MANAGEMENT POLICY

CONTENT

Section		Page
1	Introduction	3
2	Purpose	3
3	Objectives	3
3.1	Overarching objectives and standards	3
3.2	Information security	4
3.3	Records retention	4
4	Scope	4
4.1	Students and applicants	4
4.2	Functions	5
4.3	Format	5
4.4	Users	5
5	Lines of responsibility	5
6	Monitoring and evaluation	6
7	Implementation	6
8	Related policies, procedures and further reference	7
9	Definitions	7
10	Further help and advice	8
11	Policy version and History	8
Appendix 1	Student and applicant records retention policies	9
Appendix 2	Procedures for management of student and applicant records and personal data	
1	Introduction	2
2	Student applicant data	2
3	Student records and associated personal data	3
4	Records of other services provided to students	4
5	Examined and assessed student work	5
6	Alumni records and associated personal data	6
7	Security standards for student and applicant personal data	6
8	Further help and advice	8
9	Definitions	9
10	Procedures version and history	9

POLICY

1. INTRODUCTION

This policy and its underpinning procedures set out requirements and standards for the creation, management, security and retention of student and applicant records, including examined work, in all formats, together with lines of accountability.

2. PURPOSE

This policy and procedures aim to set out consistent, auditable standards for the management of records relating to applicants, enrolled and former students, including examined work, to ensure their confidentiality, integrity and availability to authorised users for as long as required by the University.

This policy aims to help the University to meet its duty of care to its students and applicants and to comply with its legal obligations including the UK Home Office regulations, the UK Data Protection Act and equivalent legislation in other jurisdictions in which the University operates.

Records must be effectively and consistently managed for all applicants and all students of the University, no matter where or how they are studying, in accordance with this policy.

As the University operates internationally, through its campuses in Dubai and in Malaysia and through arrangements with partners in other jurisdictions, the remit of this policy shall include such overseas campuses and international activities and shall pay due regard to non UK legislation that might be applicable.

Overarching objectives and specific aims and requirements relating to applicant data, student records and information, student information security and examined work, are detailed below.

3. OBJECTIVES

3.1 Overarching objectives and standards

The following common objectives apply to the management of all student and applicant records and associated information

- To maintain accurate, up to date and comprehensive records for each applicant, enrolled and former student to meet the University's operational and evidential needs
- To maintain an accurate audit trail of the service provided to each student and applicant as evidence of fair and consistent practice
- To promote consistency and reduce duplication of information across systems
- To control access to and use of confidential personal information on a "need to know" basis, to protect the privacy of individuals and manage institutional risk
- To maintain records in a format and structure appropriate to the University's operational, legal admissibility and preservation requirements
- To allow all relevant information about an individual to be retrieved readily to meet the University's needs, to facilitate the individuals' rights of access to their own personal information under the UK Data Protection Act and other privacy legislation and to comply with the requirements of the UK Home Office and other external audit and accreditation requirements

POLICY

- To follow consistent policies to retain records only as long as they are required for business purposes, destroy time-expired records as soon as they are no longer needed and ensure that records of permanent archival value are promptly transferred to the University Archive in a format appropriate to their long term access and preservation. The University retains a core record of each student permanently as evidence of their attendance and attainment.

Procedures for the management of student and applicant records and personal data, together with records retention policies and schedules, are appended to this Policy.

3.2 Information Security

The University is required to maintain appropriate technical and organisational measures to comply with the UK Data Protection Act and equivalent legislation in other jurisdictions in which the University operates. These laws set out specific obligations for the University and all agents, contractors and partners who process personal data on its behalf to:

- Protect student and applicant records and personal data from unauthorized or unlawful access, use or disclosure, and against accidental loss or destruction
- Process information about University students and applicants in accordance with their rights as data subjects under the UK Data Protection Act and other privacy laws, and the University's duty of care and service standards

In order to achieve this, staff, contractors and agents must

- have access only to such student and applicant records and related personal data as is necessary for them to fulfil their duties
- complete basic online data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles
- follow the security standards for the management of student and applicant personal data set out in the procedures supporting this policy and the University's information security policies and procedures.

All requests for personal information about applicants, current and former students must be managed in accordance with the University **Procedures for responding to requests for personal data** which underpin the Data Protection Policy [URL here].

3.3 Records Retention

Directors of Administration in Schools and Institutes and Heads of Professional Services responsible for student and applicant records and examined work will liaise with HIG to manage the confidential destruction or archival retention of these records in accordance with the University records retention policies and schedules set out in Appendix 1 and published on the HIG intranet and extranet pages.

4. SCOPE

4.1 Students and applicants

This policy applies to records and associated personal information about all applicants, current and former students across all campuses and modes of study, e.g.

- on campus (Edinburgh, Scottish Borders, Orkney, Dubai and Malaysia) students,

POLICY

- exchange and work placement students,
- students who take a year out or are under temporary suspension of studies
- students who study for Heriot-Watt University awards with Partner institutions
- Independent distance learners

4.2 **Functions**

This policy applies to records documenting the entire student lifecycle from enquiries to alumni including student recruitment, enrolment, attendance and attainment, advice and support services, fees, payments, bursaries, grants, appeals, complaints and disciplinary proceedings, verification of awards, alumni activities, subject access requests and third party requests for personal data.

4.3 **Format:**

This policy applies to all paper and electronic records which document student and applicant administration and assessment, including but not limited to those generated or held in

- The current electronic student system (SAS)
- Shadow, complementary or ancillary student records systems
- Document Upload Facility (DUF)
- SAS reporting system (OBI)
- the previous student system (Archive ISS)
- Paper and electronic student files
- Customer relationship management systems (CRM)
- Virtual Learning Environment (VLE)
- Email correspondence between academic and professional services staff and students that needs to be captured on the core student file
- Case files, database records and correspondence relating to student accommodation and support services, careers advice, counselling
- Case files and committee records relating to student discipline, appeals and complaints
- Records documenting student and applicant data subject access requests
- Records in Oracle Financials relating to charges for services to individual students

4.4 **Users:**

This policy applies to all employees, contractors and agents whose duties involve use of Heriot-Watt University student, applicant and alumni records.

5. LINES OF RESPONSIBILITY

5.1 The Secretary of the University has overall accountability for the implementation of this policy and its associated procedures, delegating executive authority as appropriate to the officers set out below.

5.2 The Academic Registrar and Deputy Secretary has senior management responsibility for and oversight of all student records.

5.3 The Director of Recruitment and Admissions is responsible for managing adherence to this policy by staff and agents involved in student recruitment.

5.4 Heads of Schools and Institutes in conjunction with their Directors of Administration and Registrars are responsible for managing adherence to this policy within their respective areas and informing the Academic Registrar and

POLICY

Deputy Secretary, Director of Governance and Legal Services and Head of Head of Heritage and Information Governance of any variance.

5.5 The Director of Governance and Legal Services has senior management responsibility for measures to support legal and regulatory compliance relating to student and applicant records.

5.6 The Head of Heritage and Information Governance is responsible for recommending policy, standards and training for the management and retention of University records and monitoring the effectiveness of these measures to meet University evidential needs, compliance with data protection and information security requirements and for archival preservation.

5.7 All academic and professional service staff, contractors and agents whose duties involve managing student and applicant records are responsible for complying with this policy:

- maintaining appropriate records, as set out in this policy and underpinning procedures
- undertaking relevant training and awareness activities provided by the University to support compliance with this policy
- ensuring that no breaches of information security result from their actions
- reporting any breach, or suspected breach of security in line with the University Information Security Incident Management Procedures.

6. MONITORING AND EVALUATION

6.1 The Academic Registrar and Deputy Secretary, Director of Governance and Legal Services and the Head of Heritage and Information Governance will have joint responsibility for organising frequent monitoring and audits of student records The outcome of each audit and any relevant issues arising between audits will be reported to the Secretary's Board, Learning and Teaching Administrators' Forum and the Information Governance and Security Group.

6.2 The policy will be reviewed every three years or more frequently as required to take account of changes to the regulatory or risk environment.

7. IMPLEMENTATION

The officers listed in section 5 above will ensure that implementation of this policy is supported by effective procedures, guidance and appropriate communications, training and awareness-raising measures. These will be designed to be applicable to all individuals and bodies who have access to information about applicants and students and tailored as required to support staff and contractors in specific roles.

POLICY

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

This policy and procedures should be read in conjunction with the student related and information security, data protection and records management policies, procedures and guidance published at

https://www.hw.ac.uk/uk/services/academic-registry/quality/learning-teaching/learning-and-teaching-policies.htm

https://www.hw.ac.uk/uk/about/policies.htm

9. DEFINITIONS

Information	The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.
Personal Data	Information in any format that relates to a living person who can be identified from that information or other information held by the University, its contractors, agents and partners or other third parties. Although the UK Data Protection Act applies only to living people, the scope of this policy also includes information about deceased former applicants and students. This is because disclosure of information about the deceased may still be in breach of confidence or otherwise cause damage and distress to living relatives and loved ones.
Sensitive Personal Data	Sensitive personal information (as defined in Section 2 of the UK Data Protection Act 1998 relating to an identifiable individual's a) racial or ethnic origin; b) political opinions; c) religious or other beliefs; d) membership of a trade union; e) physical or mental health or condition; f) sexual life; g) proven or alleged offences, including any legal proceedings and their outcome
High Risk Confidential Information	Includes a) sensitive personal data b) any other information that would cause significant damage or distress to an individual if it was disclosed without their consent, such as bank account and financial information, marks or grades c) Any privileged or proprietary information that could cause significant harm to the University through alteration, corruption, loss, misuse, or unauthorised disclosure.

POLICY

Record	A record is information, in any format, which must be retained as evidence of actions or decisions for operational or legal purposes.
Archives	Records which have been created or received by the University in the course of its activities and functions and selected for permanent preservation for their historical or evidential value, by HIG in consultation with the records creators.
Student File	Records which have been filed together in electronic or paper format to form an audit trail of the University's interaction with an individual student

10. FURTHER HELP AND ADVICE

For further information and advice about this policy and procedures contact:

Kathy Patterson
Academic Register and Deputy Secretary
Registry Services
Telephone: +44 (0)131 0131 451 3368
Email: K.Patterson@hw.ac.uk

Rachel Bourhill
Registry Officer (Enrolment)
Academic Registry, Registry Services
Telephone: +44 (0)131 0131 451 3384
Email: registry@hw.ac.uk

Ann Jones
Head of Heritage and Information Governance
Governance and Legal Services
Telephone: +44 (0)131 451 3219
Email: a.e.jones@hw.ac.uk or foi@hw.ac.uk

Brian Kelvin
Records Manager
Heritage and Information Governance
Governance and Legal Services
Telephone: +44 (0)131 451 4140
Email: b.d.a.kelvin@hw.ac.uk or: foi@hw.ac.uk

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V. 4	03.12.2013	Secretary's Board	This policy supersedes the following policies for the Management of Student Files and Records and the Records Retention Policy for Examination Scripts and Marked Course Work Revised following consultation with Learning and Teaching Administrators' Forum and Directors of Administration

POLICY

APPENDIX 1 – Student and applicant records retention policies

1. Applicant records held in SAS and Document Upload Facility (DUF)

1.1 For each successful applicant who goes on to enrol as a student

At the point of enrolment, School Directors of Administration are responsible for capturing in the official student record file all relevant information including evidential documents submitted in the course of the student's application. This will involve transferring documents from DUF into the electronic or paper record file. All documents relating to enrolled students must be transferred from DUF into the student file by the end of the academic year in which the student was enrolled as they will be deleted from DUF in an annual purge after that time.

1.2. For each applicant who does not enrol as a student

- The Student Systems Unit will delete the following applicant records from SAS and DUF in an annual purge at the start of the academic year after the year in which the applicant was seeking to enter the University. Thus, if someone applies in the academic year 2012-13 for entry in the year 2013-14 and their application is unsuccessful their record will be due for deletion in November 2014 following the final enrolment deadline. This applies:

- Where the applicant has not submitted the application and there are no associated applications or student records since 31 August in the previous academic year

- To applications which have been rejected, withdrawn or to which no offer was made by 31 August in the previous academic year; with no associated applications

- Where the applicant has not accepted and enrolled on a programme within the next academic year

- Where the applicant has accepted a place but has not enrolled or requested deferred entry

1.22 paper copies of application records

As SAS and DUF contain the evidential records of applicants, any paper copies of these records of applicants who are unsuccessful or do not enrol or request deferred entry can be confidentially destroyed in November of the academic year in which they would have enrolled.

1.3 Retention of application statistics

Prior to the annual purge, Recruitment and Admissions staff will need to export anonymised application statistics for statutory and business reporting purposes. These anonymised statistics will be retained permanently.

POLICY

2. Student Records in SAS and ISS:

Student data in SAS and ISS constituting the core permanent records specified in section **4** below will be retained permanently as archival records.

The Head of Heritage and Information Governance, the Director of Information Services and the Academic Registrar and Deputy Secretary will agree processes and standards for the permanent curation of these datasets and associated core student files held in electronic format in accordance with the University Digital Preservation Policy.

3. Management of student files while current and transfer to the University Archive

Each School is responsible for following the Procedures for Managing Student Records to maintain an individual file for each student as part of a comprehensive record of student progress and attainment. Each student file, whether in paper or electronic format, should be structured into sub-folders to distinguish between

- records that must be retained permanently; and
- records that must be destroyed when they are no longer required in accordance with the records retention schedules in order to comply with the Data Protection Principle that personal data must be retained no longer than necessary

School Directors of Administration are responsible for transferring student files to Heritage and Information Governance for preservation in the University Archive **one year** after the student has left the University. These officers will liaise with the Head of Heritage and Information Governance to confirm the format of the records to be transferred and the method of transferring electronic records.

Information in categories 1-15 form the core permanent record which will be retained in the University Archive for posterity. It is essential that these are either originals or reliable and authentic copies.

The remaining information listed comprises records to be destroyed 6 years after the student has left the University. Before transferring student files to HIG, School Directors of Administration will ensure that all such information is filed in a separate and clearly identified sub-folder of the main file or in a separate sealed envelope. HIG staff will then remove these sub-folders or envelopes and arrange for their confidential destruction 6 years after the student has left the University.

4. Definition of core, permanent archival records and records to be retained for a limited period

Core permanent archival records

1. UCAS or other application form and associated supporting information submitted as evidence of identity and eligibility to enrol, e.g. Records of Prior Accreditation e.g. copies of academic award certificates; academic references; the signature of the applicant, passport/visa documents, Confirmation of Acceptance for Studies (CAS) letters, where appropriate. For students on Academic Technology Approval Scheme, ATAS clearance certificate

2. Evidence of completed enrolment for each academic year or stage of programme including at least one photograph taken as part of the enrolment process

3. Examination results in SAS, including a breakdown of marks and grades for each course. An audit trail of the issue of results to each student. A copy of (or audit trail) of the final year results letter including the date of issue and the final correspondence addresses to which the letters were sent

POLICY

4. Records of examination resits, examination failure and unsatisfactory progress, including any associated correspondence. Retain correspondence relating to resit undertaken at an overseas institution, where applicable. This confirms permission to undertake resit abroad, which is only permitted as an exceptional arrangement.

5. Records of withdrawals and transfers between programmes and campuses, including correspondence with the student and Change of Course/Programme Forms.

6. Correspondence relating to appeals

7. Confirmation of qualification awarded and date of award.

8. Correspondence relating to the award of medals and prizes, where applicable.

9. Higher Education Achievement Record (HEAR) for each student, if implemented

10. The outcome of a disciplinary hearing where it results in a student being required to withdraw or have their award rescinded

For postgraduate students only

11. Correspondence relating to the appointment of Postgraduate External Examiner(s) for individual PhD and MPhil candidates

12. Submission of Postgraduate Thesis and Abstract of Thesis Forms.

13. Reports from Postgraduate Internal and External Examiners.

14. Reports on the Re-submission of Postgraduate Thesis, where applicable.

15. Re-submission Reports from Postgraduate Internal and External Examiners, where applicable.

Records to be destroyed 6 years after the student has left the University

1. Confirmation of ability to pay fees, submitted as part of the application process

2. Records documenting attendance, including compliance with mandatory Home Office Tier 4 contact points where relevant

3. Information on any matter relating to discipline which does not result in a student being required to withdraw or have their award rescinded, including correspondence with the student

4. Records documenting the handling of complaints made by individual students

5. Information on health and welfare, including correspondence with the student

6. Mentoring records (provided by academic mentors at year end) including PhD Annual Appraisals

7. Home and semester addresses and contact information, other than those provided at the point of application and the last known address at the point of the award; next of kin contact details

POLICY

5. Sharing of student personal data post- studies for alumni relations and statistical purposes

Unless leavers have asked not to have their personal data shared for this purpose, at graduation, the Academic Registry will provide a report from SAS with the names, awards, postal and email addresses of graduates for

1. The Development and Alumni Office in order to enrol them in the Watt Club; the University Alumni Association. .

2. The Careers Advisory Service for disclosure to the Scottish Government to seek students' participation in the Higher Education Statistics Agency (HESA) Destinations of Leavers from Higher Education (DLHE) survey

6. Retention of examined work

6.1 Examination papers

The Head of Heritage and Information Governance and the Deputy Principal (Learning, Teaching and Quality) will agree a process with the Academic Registrar and Deputy Secretary and the Directors of Administration and Registrars of each School and Institute for preserving, as an archival record of standards of assessment, a representative sample of the examination papers and model answers for each academic discipline, reflecting changes in course curriculum over time.

By agreement with the Deputy Principal (Learning, Teaching and Quality) Schools will retain and make available local copies of all examination papers and model answers, where provided by the academic staff (with the exception of the answers to multiple choice questions which are reused over several diets) for 3 – 5 years where these remain relevant, dependent on changes to the curriculum over this period.

6.2 PhD and MPhil Theses

Until awards have been approved by the Senate, PhD theses, once submitted, will be retained by the Academic Registry. Following approval of awards, the Academic Registry will transfer theses to the University Library. PhD Theses will be retained permanently in the Research Output Service (ROS, the University's institutional repository for published research outputs) and will be publicly available through ROS and in the British Library .

Taught MPhil. Dissertations should be retained for one year following successful completion and award and can then be destroyed or retained for reference purposes in Schools. HIG may liaise with Schools and Information Services to select a representative sample for the University Archive.

6.3 Examination Scripts and other Examined Work

These may be destroyed 4 months after the decision of the relevant Progression/Award/ Resit Board or when the deadline for student appeals for the relevant diet has passed and should be retained for no more than a year.

6.4 Appeals

Where a student has lodged an appeal or raised a complaint relating to an academic matter or is involved in a disciplinary case relating to an academic matter, where practicable the School Director of Administration will retain a representative sample of the examination scripts/assessed work for the cohort of students in the relevant diet until the appeal has been resolved.

POLICY

6.5 Sampling for accreditation of awards by professional bodies

Each School will agree a protocol with their accrediting bodies to retain a sample, only, of between 5 and 20% of scripts or other examined work for the relevant quality review by that body. Samples of examined work retained for this purpose and other records documenting the conduct and results of external reviews and audits of teaching quality and standards will be retained until the following review and destroyed thereafter. The Academic Registrar and Deputy Secretary and HIG will be informed of the retention protocol as required for each accrediting body.

The Academic Registry will communicate clearly to students that samples of their work may be retained and reviewed by third parties for quality assurance purposes. e.g. by placing the following statement in the relevant sections of the University website and programme handbook:

"Completed examination scripts and course work submitted for assessment will be held securely by your School for a limited time in accordance with the University's records retention policy and destroyed confidentially. Your School may retain a sample of completed examination scripts and assessed work for a longer period to meet the review requirements for professional bodies. For further information please contact your programme administrator or the University's Data Protection Officer."

Examination scripts/assessed work will be retained by Schools and Institutes and destroyed confidentially at the end of their retention period.

7.0 Further information about records retention policies

More detailed retention schedules for records documenting the student and applicant lifecycle will be published here:

Intranet for staff users
https://heriotwatt.sharepoint.com/sites/gals-informationgovernance

Extranet: https://www.hw.ac.uk/uk/services/information-governance.htm

POLICY

Procedures for the management of student and applicant records

In support of the Student Records Management Policy

PROCEDURES

HERIOT-WATT UNIVERSITY

PROCEDURES for the management of student and applicant records

CONTENT

Section		Page
1	Introduction	2
2	Student applicant data	2
3	Student records and associated personal data	3
4	Records of other services provided to students	4
5	Examined and assessed student work	5
6	Alumni records and associated personal data	6
7	Security standards for student and applicant personal data	6
8	Further help and advice	8
9	Definitions	9
10	Procedures version and history	9

PROCEDURES

1. INTRODUCTION

These procedures support the Student Records Management Policy by setting out in more detail a specification of standards and requirements to ensure that records documenting the University's interaction with applicants, students and alumni are fit for purpose and meet evidential and legal requirements.

Schools and professional services must ensure that their electronic and paper records systems meet the standards specified within this policy, procedures, appendices and associated guidance.

2. STUDENT APPLICANT DATA

2.1

The Director of Recruitment and Admissions will agree responsibilities and procedures for the management and security of student applicant records and associated personal data with the Heads and Directors of Administration in Schools and Institutes.

These officers will agree record keeping standards and protocols for all undergraduate and postgraduate student recruitment to

- Provide an agreed chain of custody to retain an accurate record of each application and its outcome.
- Demonstrate that a fair and consistent recruitment process has been followed in each case and where relevant, meet the requirements of the UK Home Office
- Ensure that all relevant information about each successful applicant who goes on to matriculate as a student is captured in the core student record, including evidential documents submitted in the course of the application
- Implement the timeous destruction of application data where the applicant is unsuccessful or does not enrol, in accordance with the University records retention policies

2.2 The scope of the standards and protocols will take account of all records and information documenting the application process including

- Enquiries from potential applicants
- Applications submitted through UCAS
- Application forms submitted directly to the University online or in paper format
- Associated evidential records such as certificates of prior awards, reference, passport and visa records and financial guarantees
- Correspondence between University staff, contractors and agents and applicants concerning the progress of their applications and decisions made

2.3 Contractual agreements and induction for recruitment agents and contractors will incorporate these record keeping standards and security controls so that agents will have a clear understanding of their responsibilities as data processors for the University.

2.4 The Student Recruitment Customer Relationship Management System will form the

PROCEDURES

evidential record of the correspondence between each prospective applicant and hthe University, from initial enquiry to acceptance of offer

2.5 From the point that the University receives an application from UCAS, or a potential student begins the process of applying online using my Heriot-Watt, a unique applicant record is created in the electronic student records system, SAS. From this point, SAS and its associated Document Upload Facility become the evidential record documenting the progress and outcome of each application.

3 STUDENT RECORDS AND ASSOCIATED PERSONAL DATA

3.1 The Academic Registrar and Deputy Secretary and each Head and Director of Administration in Schools will jointly implement the following agreed standards for management of student records and associated personal data.

This section focuses on the management of the core student record in SAS and in the individual student files created by Schools. Standards for the management of student records created in the course of delivering professional services or adjudicating complaints or disciplinary proceedings can be found in section 4 below.

3.2 The Academic Registry and each School and Institute will create and maintain a comprehensive student record of the progress and attainment for each student.

This comprehensive student record has the following components:

1. The primary student record is held within the electronic student records system (SAS) and its predecessor ISS. It is recognised that SAS and ISS do not contain all of the evidential records that must be retained for each student and that therefore it must be supplemented by a paper or electronic file for each student.

2. Therefore in addition one student file will be designated and maintained in paper or electronic form as part of the official evidential record for each student. This file will be held locally within the School and campus in which the student is based. For those students who are based off campus or study with Approved Learning Partners the School will maintain the evidential file. Each file must be available for access by staff from the Academic Registry when required for the normal conduct of their duties.

Together the SAS record and the individual student file comprise the comprehensive student record of progress and attainment.

3.3 Each School Director of Administration and Registrar is responsible for ensuring that acceptable mechanisms for paper and electronic file management are in place within their School to maintain the confidentiality, integrity and accessibility of all student files until they are transferred to the University Archive.

3.4 Appendix 1 of the Student Records Management Policy contains a list of records to be retained in the student file, divided into Permanent Records and records to be retained for a limited time.

3.5 It is recommended that each student file should be structured into sub-folders to distinguish between

- Permanent records to be retained permanently as part of the University Archive
- Records to be kept for a limited period only and then destroyed confidentially 6 years after each student has gained his/her final award or left the University.

If documents are scanned and held electronically, particular care must be taken to avoid combining permanent and time limited records in the same electronic file. This is necessary to comply with the Data Protection Principle that personal data must be kept no longer than necessary.

If paper files are kept in chronological order while they are current, the separation of permanent and time limited records can take place at the point that the student graduates or leaves the University as long as the records have been subdivided in this way before transfer into the University Archive

3.6 Academic staff must pass all correspondence with students about their progress to the School administrators for filing within the evidential student file. Academic staff should not therefore retain any records, correspondence or paperwork on individual students, other than 'live' working documents, which should be transferred to the official evidential student file as soon as practicable.

3.7 If the evidential student file is held in paper format, the School Director of Administration and Registrar may for ease of reference set up a corresponding electronic file for each student containing records that are not held in SAS but which were created electronically or received from the student in electronic format, while the student is enrolled at the University. Except for the above reference copy of the paper or electronic file, there must be no shadow student files or papers held in a separate location in Schools. When the student has left the University the reference copy can then be confidentially destroyed.

3.8 Where a School designates the electronic student file as the official evidential record, individual records should be saved in pdf or another read only format to reduce the risk of them being accidently changed or overwritten. Schools wishing to store or transfer electronic student records should seek advice from Heritage and Information Governance on standards and guidance for evidential electronic recordkeeping.

3.9 Where a student has entered the UK on a Tier 4 visa, his or her file is subject to regular audit to demonstrate compliance with Home Office immigration rules. A file copy of the completed Tier 4 Check Sheet should be added to the front of the file together with copies of the essential documents i.e. certificates, transcripts, proof of English language, copies of passports/visas etc.

4 RECORDS OF OTHER SERVICES PROVIDED TO STUDENTS

4.1 Each professional service which provides services to students needs to maintain an accurate and comprehensive case file or equivalent customer record documenting its interaction with each individual student. The format and scope of each case file or recording system will vary according to the service provided but in all cases should allow staff to retrieve all relevant information that the service holds about the individual student.

4.2 The Academic Registrar and Deputy Secretary, the Heads of Student Support and Accommodation and the Careers Service will agree and jointly implement standards

PROCEDURES

for management of student case files and associated personal information created in the course of providing student services and Academic Registry functions. The Student Service Centre Manager will liaise with managers in the Academic Registry, Finance Office and Campus Services to agree and implement standards for management of records created in the Student Service Centre. Other professional service Directors and their service heads will agree standards for management of student records created in the course of delivering their services.

4.3 Record keeping standards and retention policies include but are not confined to the following services and functions:

- Academic Registry including Student Systems Unit
- Student Service Centre
- Payment of tuition and accommodation fees, debt management, library fines and other charges
- Financial sponsorship, bursaries, scholarships
- Accommodation
- Counselling and support
- Disability Service advice and support
- Careers advice and mentoring
- Financial advice, support and Hardship Grant awards
- International student advice
- Chaplaincy Service
- Disciplinary proceedings
- Student appeals
- Student complaints
- Referrals of individual students to the Health Centre
- Liaison with Heriot-Watt University Students Union e.g. to confirm students' eligibility to vote and use facilities
- Centre for Sport and Exercise membership
- Information Services: use of Library and IT facilities
- Heritage and Information Governance: e.g. student access to University collections, FOI and data subject access requests

5 EXAMINED AND ASSESSED STUDENT WORK

Directors of Administration in Schools and Institutes and the designated officers in Dubai and Malaysia will store work submitted by students for examination and assessment securely and retain it only so long as it is required for business purposes to:

- assess and award grades; in accordance with internal and external examination procedures
- support students' rights to feedback and transparency in understanding how examination marks and grades have been awarded and to exercise their rights to appeal within the deadlines specified in Regulation 36 (Student Appeals);
- provide a sample only as evidence for quality assurance and professional review and meet the University's obligations to external accrediting bodies

PROCEDURES

6. ALUMNI RELATIONS

The Director of Development and Alumni Relations will agree and implement standards for management of alumni records and associated personal information, including:

- Records held in the Alumni customer relationship management database, Raisers' Edge
- Alumni events
- Sponsorship and donations
- Disbursement of funds to current students

7. SECURITY STANDARDS FOR STUDENT AND APPLICANT PERSONAL DATA

7.1 Members of staff, contractors and agents must have access only to such student and applicant records and related personal data as is necessary for them to fulfil their duties.

7.2 The Academic Registrar and Deputy Secretary is responsible for authorising user access to SAS and its associated databases and interfaces [including DUF, Faculty Self Service and OBI] and for auditing access every three months as recommended by the University's Internal Auditors.

7.3 All staff, contractors, agency staff and agents whose roles require access to student or applicant records and associated personal data in SAS or in shared paper and electronic filing systems will undertake mandatory information security induction and refresher training.

7.4 The Head of Heritage and Information Governance will lead the development of information governance training and awareness, working closely with the Academic Registrar and Deputy Secretary, the Director of Information Services and Organisational Development and other colleagues in Schools and Professional Services to provide relevant and practical guidance and advice.

7.5 School Directors of Administration and Directors of Professional Services are responsible for determining which roles may require staff to work off campus and have remote access to sensitive personal data or other high risk personal information about applicants or students. Directors are responsible for working with their IT providers to put in place safe remote working arrangements including the University Virtual Private Network (VPN) or encrypted portable media in accordance with the University's information security policies.

7.6 Electronic student files, case files or service records about identifiable students must be held on restricted access shared drives or information management systems. Access permissions to these drives or systems must be authorised by the relevant School Director of Administration and Registrar, or Director of Professional Service, with assistance from a designated member of staff.

7.7 Paper student files must be stored in secure locked cabinets managed by the School Director of Administration and Registrar, with assistance from a designated member of staff. The Academic Registrar and Deputy Secretary must be informed of the names of these designated individuals and will arrange annual audits of access and spot checks.

PROCEDURES

7.8 Student files should, wherever possible, be viewed in the room where the records are held. All files removed from the secure storage facility must be signed out and in, and must be returned as soon as possible, with follow-up by the designated responsible person and the School Director of Administration and Registrar if not returned within one week.

7.9 All users with access to student records and other confidential information need to follow the following basic security principles

7.10 Keep personal data and other confidential information securely:

- Don't leave paper records containing confidential information where others can see them when they come into your office. Keep them In locked cabinets or drawers: remove the keys and keep them securely
- Protect electronic documents with strong passwords combining upper and lower case letters and numbers or symbols
- Lock your computer screen [press Windows key and L] or log out when you are leaving your desk
- Use the University VPN if you need to access confidential information for work away from the office
- Never take personal or confidential data off campus e.g. on smartphones, tablets, laptops or memory sticks unless it is encrypted
- Don't keep data on your computer hard drive. Use your "home" drive or a restricted access folder in your shared drive as these are backed up.
- Protect your Heriot-Watt University passwords and don't share with others.

7.11 Take control of your communications

- Use only your University email account for work emails.
- If you have to send confidential information by email, encrypt or password protect it
- Double check your recipient's email address before you press the Send button to ensure the message gets to the right person and not their namesake
- Don't respond to email requests for your password or bank details
- Be cautious about opening email attachments even from colleagues– if in doubt scan for viruses.
- If you use social media for work, use the privacy settings to protect personal and confidential data. Check that you don't surrender Intellectual Property Rights (IPR) to the service provider.
- Use only cloud providers recommended by your IT service and Heritage and Information Governance for remote storage of personal data and other confidential information. Services such as Dropbox are not secure and the University bears all risk and liability for data loss. Keep backup copies of important records on University systems as external services can and do disappear. Before using an externally managed service, ensure that the University has a data processor agreement in place with the provider, including arrangements for file recovery and business continuity

7.12 Destroy information confidentially when no longer needed.

- Use the University's records retention schedules which set out what information needs to be kept for how long. Ask us for advice and help.
- Never dispose of information which is not intended for publication in the waste or recycling bin. Use your School/Service shredder or a secure destruction service for confidential records instead.
- Ensure that information is completely erased from obsolete computer hardware and portable storage devices. Deleting the data is not sufficient. Ask your local IT team for the best method of removing data permanently.

7.13 Report information security incidents and lost or stolen devices immediately
Contact IThelp@hw.ac.uk or Security Control on +44 (0)131 451 3500

8. FURTHER HELP AND ADVICE

For further advice and assistance contact

Kathy Patterson
Academic Register and Deputy Secretary
Registry Services
Telephone: +44 (0)131 0131 451 3368
Email: K.Patterson@hw.ac.uk

Rachel Bourhill
Registry Officer (Enrolment)
Academic Registry, Registry Services
Telephone: +44 (0)131 0131 451 3384
Email: registry@hw.ac.uk

Ann Jones
Head of Heritage and Information Governance
Governance and Legal Services
Telephone: +44 (0)131 451 3219
Email: a.e.jones@hw.ac.uk or foi@hw.ac.uk

Brian Kelvin
Records Manager
Heritage and Information Governance
Governance and Legal Services
Telephone: +44 (0)131 451 4140
Email: b.d.a.kelvin@hw.ac.uk or: foi@hw.ac.uk

9. DEFINITIONS

Information	The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.

PROCEDURES

Personal Data	Information in any format that relates to a living person who can be identified from that information or other information held by the University, its contractors, agents and partners or other third parties. Although the UK Data Protection Act applies only to living people, the scope of this policy also includes information about deceased former applicants and students This is because disclosure of information about the deceased may still be in breach of confidence or otherwise cause damage and distress to living relatives and loved ones.
Sensitive Personal Data	Sensitive personal information (as defined in Section 2 of the UK Data Protection Act 1998 relating to an identifiable individual's a) racial or ethnic origin; b) political opinions; c) religious or other beliefs; d) membership of a trade union; e) physical or mental health or condition; f) sexual life; g) proven or alleged offences, including any legal proceedings and their outcome
High Risk Confidential Information	Includes a) sensitive personal data b) any other information that would cause significant damage or distress to an individual if it was disclosed without their consent, such as bank account and financial information, marks or grades c) Any privileged or proprietary information that could cause significant harm to the University through alteration, corruption, loss, misuse, or unauthorised disclosure.
Record	A record is information, in any format, which must be retained as evidence of actions or decisions for operational or legal purposes.
Archives	Records which have been created or received by the University in the course of its activities and functions and selected for permanent preservation for their historical or evidential value, by HIG in consultation with the records creators.
Student File	Records which have been filed together in electronic or paper format to form an audit trail of the University's interaction with an individual student

9. PROCEDURES VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
4	xx.xx.xxxx		