Data Protection Policy

December 2021

Approving authority:	Court
Consultation via:	Audit and Risk Committee, University Executive, Global Operations Executive, Global Information Governance and Data Protection Committee
Approval date:	16 December 2021
Effective date:	16 December 2021
Review period:	Two years from date of approval
Responsible Executive:	University Secretary
Responsible Office:	Information Governance Division, Governance and Legal Services

POLICY

HERIOT-WATT UNIVERSITY
DATA PROTECTION POLICY
CONTENTS

POLICY

1. INTRODUCTION

Heriot-Watt University is an international community of learning, and personal interaction is at the heart of our mission to create and exchange knowledge for the benefit of society. The University's need to communicate and share personal data worldwide also presents significant data protection risks.

As members of a global interconnected university, we need to ensure that everyone enjoys the same high standards of privacy in their interactions with us wherever in the world they may be. This aligns with our Strategy and Values. This means that we will comply with the highest legal standard applicable unless the law in a particular country requires us to make an exception, which we then document and explain to the individuals concerned. The benchmark legal standard is the European Union General Data Protection Regulation (GDPR) as applied in UK law.

The University Group must comply with relevant legislation protecting privacy rights in every jurisdiction where the University operates. As the University and its constituent legal entities are UK Data Controllers, and also Data Processors for certain activities, the territorial scope of UK Data Protection legislation, and therefore of this policy, applies to all processing of personal data by and for the University, regardless of where the processing takes place.

As of 1 January 2021, the European Union (EU) General Data Protection Regulation (GDPR) has been embedded into UK law as the UK GDPR alongside the revised UK Data Protection Act, 2018 (DPA) and Privacy and Electronic Communications Regulations 2003 (PECR).

In addition, we must comply with the European Union (EU) General Data Protection Regulation (GDPR) in relation to personal data collected before 31 December 2020 and when offering goods and services to people in the EU or monitoring their behaviour in the EU.

In Dubai we apply the UK GDPR, DPA and PECR together with the United Arab Emirates Federal Data Law that protects personal privacy.

We comply with the Malaysia Personal Data Protection Act 2010, alongside the UK GDPR, DPA and PECR for activities involving our Malaysia campus.

These data protection laws require the University to protect personal information and control how it is used in accordance with the legal rights of the data subjects - the individuals whose personal data is held.

All data subjects are entitled to know:

- Their rights under data protection law and how to use them,
- What the University is doing to comply with its legal obligations under data protection law.

POLICY

Misuse of personal data, through loss, disclosure, or failure to comply with the Data Protection Principles and the rights of data subjects, may result in significant legal, financial and reputational damage. This may include penalties of up to £17.5 million or 4% of worldwide annual turnover for serious breaches of the law, claims for compensation and loss of recruitment and research income.

In order to manage these risks, this policy sets out responsibilities for all managers, employees, contractors, and anyone else who can access or use personal data in their work for the University.

2. PURPOSE

2.1 This policy and its supporting procedures and guidance support University compliance with its obligations as a Data Controller and where applicable, a Data Processor under data protection law.

The University is responsible for, and must be able to demonstrate, compliance with the following Data Protection Principles ("accountability").

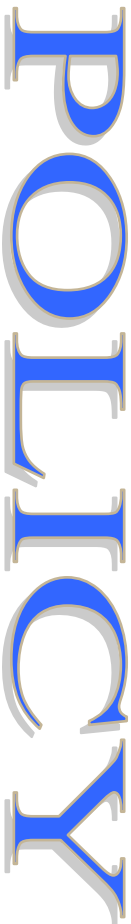
In summary, these state that personal data shall be:

- Processed lawfully, fairly and in a way that is transparent to the data subject ("lawfulness, fairness and transparency"),
- Collected or created for specified, explicit and lawful purposes and not be further processed in a manner that is incompatible with those purposes ("purpose limitation"),
- Adequate, relevant and limited to what is necessary for those purposes ("data minimisation"),
- Accurate and kept up to date ("accuracy"),
- Retained in a form that can identify individuals for no longer than is necessary for that purpose ("storage limitation"),
- Kept safe from unauthorised access, processing, accidental or deliberate loss or destruction ("integrity and confidentiality"),

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is compatible with the purpose and storage limitation principles, subject to appropriate safeguards for the rights and freedoms of the data subjects.

Under data protection law the University must also:

- Proactively inform data subjects about its data processing activities and their rights under the law,
- Meet its legal obligations as a data controller or processor, including data protection by design and default, data protection impact assessment, maintaining records of processing activities, measures



to ensure the security of processing, handling of data breaches; designation and role of the Data Protection Officer,

- Allow personal data to be transferred to other countries only if appropriate safeguards are in place to maintain the same level of protection for the privacy rights of the data subjects concerned.

2.2 This policy sets out a framework of governance and accountability for data protection compliance across the University. It forms part of the University Information Security Management System (ISMS). This incorporates all policies and procedures that are required to protect University information by maintaining:

- Confidentiality: protecting information from unauthorised access and disclosure,
- Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorised amendment or deletion,
- Availability: ensuring that information and associated services are available to authorised users whenever and wherever required,
- Resilience: the ability to restore the availability and access to information, processing systems and services in a timely manner in the event of a physical or technical incident.

3. OBJECTIVES

The University will apply the Data Protection Principles and the other requirements of data protection law to the management of all personal data throughout the information life cycle by adopting the following policy objectives.

3.1 Process personal data fairly and lawfully

This means that we will:

- Only collect and use personal data in accordance with the lawful conditions set down under the UK GDPR;
- Document each condition we rely on; maintain this information within a formal set of Records of Processing Activities; regularly review and update these records and make them available to the Information Commissioner's Office, other supervisory authorities and data subjects on request;
- Treat people fairly by using their personal data for purposes and in a way that they would reasonably expect;
- Ensure that if we collect someone's personal data for one purpose e.g. to provide advice on study skills, we will not reuse their data for a different purpose that the individual did not agree to or expect e.g. to promote goods and services for an external supplier;

POLICY

- Rely on consent as a condition for processing personal data only where:
    - We first obtain the data subject's specific, informed and freely given consent, and
    - The data subject gives consent, by a statement or a clear affirmative action that we document, and
    - The data subject can withdraw their consent at any time without detriment to their interests.

Where we are relying on substantial public interest to process special categories of personal data or criminal offences personal data we must have an appropriate policy document in place specifying

- Which condition we rely on
- How we comply with the data protection principles
- How long we retain the data

3.2 Inform data subjects what we are doing with their personal data

This means that, at the point that we first collect their personal data, we will explain to data subjects in a clear, concise and accessible way:

- The identity and contact details of the University and the Data Protection Officer,
- What personal data we collect,
- For what purposes we collect and use their data,
- What lawful conditions we rely on to process data for each purpose and how this affects their rights,
- Whether we intend to process the data for other purposes and their rights to object,
- The sources from which we obtain their data, where we have received the data from third parties,
- Whether we use automated decision making, including automated profiling, and if so the impact on data subjects and their rights to object,
- Whether they need to provide data to meet a statutory or contractual requirement and if so, the consequences of not providing the data,
- Our obligations to protect their personal data,
- To whom we may disclose their data and why,
- Which other countries we may send their data to, why we need to do this and what safeguards apply in each case,
- Where relevant, what personal data we publish and why,

POLICY

- How data subjects can update the personal data that we hold,
- How long we intend to retain their data,
- How to exercise their rights under data protection law.

We will publish this information on our website and where appropriate in printed formats. We will review the content of these Privacy Notices regularly and inform our data subjects of any significant changes that may affect them.

We will provide simple and secure ways for our students, staff and other data subjects to update the information that we hold about them such as home addresses.

Where we process personal data to keep people informed about University activities and events, we will provide in each communication a simple way of opting out of further marketing communications.

In these ways we will provide accountability for our use of personal data and demonstrate that we will manage people's data in accordance with their rights and expectations.

3.3 Uphold individual's rights as data subjects

This means that we will uphold their rights to:

- Obtain a copy of the information comprising their personal data, free of charge within one month of their request, only extending this by the permitted deadline of two further months in the case of complex or voluminous requests,
- Have inaccurate personal data rectified and incomplete personal data completed,
- Have their personal data erased when it is no longer needed, if the data have been unlawfully processed or if the data subject withdraws their consent, unless there is an overriding legal or public interest in continuing to process the data,
- Restrict the processing of their personal data until a dispute about the data's accuracy or use has been resolved, or when the University no longer needs to keep personal data but the data subject needs the data for a legal claim,
- Data portability; where a data subject has provided personal data to the University by consent or contract for automated processing and asks for a machine-readable copy or have it sent to another data controller,
- Object to and prevent further processing of their data for the University's legitimate interests or public interest unless the University can demonstrate compelling lawful grounds for continuing,

POLICY

- Prevent processing of their data for direct marketing,
- Stop the University processing data obtained for online services such as social media, where consent for the processing was previously given by or on behalf of a child, who withdraws their consent,
- Object to decisions that affect them being taken solely by automated means,
- Claim compensation for damages caused by a breach of data protection law.

3.4 Apply "data protection by design and default" principles to all our personal data processing

This means that we will:

- Integrate the data protection principles into functional design and implementation from the outset of every project or initiative that involves processing personal data, and in managing upgrades or enhancements to systems and processes used to process personal data, using proportionate privacy and information risk assessment, and where appropriate, data protection impact assessment, to identify and mitigate privacy risks at every stage,
- Apply a "privacy first" approach to any default settings of systems and applications,
- Adopt data minimisation: we will collect, disclose and retain the minimum personal data for the minimum time necessary for the purpose,
- Anonymise personal data wherever necessary and appropriate, e.g. when using it for statistical purposes, so that individuals can no longer be identified,
- Audit online services likely to be accessed by children to ensure that they comply with relevant provisions of the UK Information Commissioner's Office statutory Age Appropriate Design Code

3.5 Protect personal data

This means that we will use appropriate technical and organisational measures to:

- Control access to personal data so that staff, contractors and other people working on University business can only see such personal data as is necessary for them to fulfil their duties,
- Require all University staff, contractors, students and others who have access to personal data in the course of their work to complete basic data protection training, supplemented as appropriate by procedures and guidance relevant to their specific roles,

POLICY

- Set and monitor compliance with security standards for the management of personal data as part of the University's wider framework of information security policies and procedures,

- Reduce risks of disclosure by pseudonymising personal data where possible,

- Provide appropriate tools for staff, contractors, students and others to use and communicate personal data securely when working both on-campus and away from the University, for instance through provision of secure online platforms, a Virtual Private Network, encryption and cloud solutions,

- Use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will comply with data protection law and ensure the protection of the rights of the data subject. This means we will take all reasonable steps to obtain evidenced assurance that all suppliers, contractors, agents and other external parties who process personal data for the University will enable us to comply with the data protection principles and the rights of data subjects and comply with auditable security controls to protect our data, enter into our Data Processor Agreements, or equivalent contracts that embed all the controller and processor obligations under the law,

- Maintain Data Sharing Agreements with educational partners and other external bodies with whom we may need to share personal data to deliver academic programmes, shared services or joint projects and activities to ensure proper governance, accountability and control over the use of such data,

- Where transferring personal data to another country outside the UK use adequacy assessment where necessary, apply data minimisation, and put in place appropriate agreements and auditable security controls to provide the safeguards necessary to maintain privacy rights,

- Ensure that our students are aware of how data protection law applies to their use of personal data in the course of their studies or research and how they can take appropriate steps to protect their own personal data and respect the privacy of others,

- Manage all data subject requests and third-party requests for personal information about staff, students and other data subjects in accordance with our Procedures for managing personal data requests

- Make appropriate and timely arrangements to ensure the confidential destruction of personal data in all media and formats when it is no longer required for University business.

POLICY

3.6 Provide appropriate legal and organisational safeguards to maintain privacy rights and data flows when sharing personal data with organisations in other countries

This means that when considering transfer of personal data or two-way data sharing with organisations in countries outside the UK and European Economic Area we will:

- Check if the recipient country has received a UK or European Commission Adequacy decision indicating that the country provides adequate protections for the privacy rights and freedoms of data subjects,

- Before sharing personal data with a recipient in a country without an Adequacy decision, complete an international transfer risk assessment, apply data minimisation and security controls and put in place a legally binding and enforceable international data transfer agreement with the recipient to provide 'appropriate safeguards' for the rights of the data subjects whose personal data is being transferred including enforceable rights and effective remedies for the individuals concerned. This agreement may include the UK Information Commissioner's Standard Data Protection Clauses for international data transfers or comprise a legally binding and enforceable instrument between two public authorities or bodies,

- Provide sufficient guarantees to organisations in other countries that wish to transfer personal data to the University of our organisational and technical measures to comply with data protection law and enter into a legally binding and enforceable agreement with that organisation to provide 'appropriate safeguards' for the rights of the data subjects whose personal data is being transferred including enforceable rights and effective remedies for the individuals concerned.

3.7 Retain personal data only as long as required

This means that we will:

- Apply the University records retention policies to keep records and information containing personal data only so long as required for the purposes for which they were collected.

Then, in line with the retention policy recommendations, we will:

- Destroy records securely in a manner appropriate to their format; OR

- Transfer them by arrangement with the Information Governance Division in Governance and Legal Services to our records storage contractor for a limited period where required for legal and evidential purposes; OR

POLICY

- Transfer the records by arrangement to the University Archivist, Information Services, for archiving in the public interest, scientific or historical research purposes or statistical purposes.

Some University records containing personal data are designated for permanent retention as archives or for scientific, historical and statistical purposes. When managing access to archives containing personal data we will apply appropriate technical and organisational measures to safeguard the rights and freedoms of the data subjects concerned:

- Apply exemptions to public rights of access to information as appropriate in accordance with the data subjects' rights to privacy,
- Redact personal data, e.g. by pseudonymisation,
- Withhold access to specific categories of record, such as student records, for the lifetime of the student and their identifiable next of kin.

3.8 Manage any breaches of data security promptly and appropriately

This means that we will take all necessary steps to reduce the impact of incidents involving personal data by following the University's Information Security Incident Management Policy and Procedures.

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will liaise with the UK Information Commissioner's Office and report the breach, in line with regulatory requirements, within 72 hours of discovery. The Data Protection Officer will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

4. SCOPE

4.1 What information is included in the Policy

This policy applies to all personal data created or received in the course of University business in all formats, of any age. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone.

4.2 Who is affected by the Policy

Data subjects

These include, but are not confined to: prospective applicants, applicants to programmes and posts, current and former students, alumni, current and former employees, family members where emergency or next of kin contacts are held, casual and other contingent workers, workers employed through temping agencies, members of the Court and members of the Committees of the Court, research subjects, external researchers, visiting scholars and volunteers, potential and actual donors, customers, conference delegates, people making requests for information or enquiries,

POLICY

complainants, professional contacts and representatives of funders, partners and contractors.

Users of personal data

The policy applies to anyone who obtains, records, can access, store or use personal data in the course of their work for the University. Users of personal data include employees and students of the University, contractors, suppliers, agents, University partners and external researchers and visitors.

4.3 Where the Policy applies

This policy applies to all locations from which University personal data is accessed including home and mobile use.

As the University operates internationally, through its campuses in Dubai and in Malaysia and through arrangements with partners in other jurisdictions the remit of the policy shall include such overseas campuses and international activities and shall pay due regard to applicable legislation in each relevant country.

5. LINES OF RESPONSIBILITY

5.1 All users of University information are responsible for

- Completing relevant training and awareness activities provided by the University to support compliance with this policy,
- Taking all necessary steps to ensure that no breaches of information security result from their actions,
- Reporting all suspected information security breaches or incidents promptly to ISHelp@hw.ac.uk so that appropriate action can be taken to minimise harm,
- Informing the University of any changes to the information that they have provided to the University in connection with their employment or studies, for instance, changes of address or bank account details.

5.2 The Principal and Vice–Chancellor, as the Chief Executive Officer of the University, has ultimate accountability for the University's compliance with data protection law.

5.3 The University Secretary has senior management accountability for information governance and for ensuring that the Data Protection Officer is given sufficient autonomy and resources to carry out their tasks effectively.

5.4 The Global Director of Governance and Legal Services has senior management responsibility for information governance within the University.

POLICY

5.5 The Head of Information Governance, as Data Protection Officer is responsible for:

- Informing and advising senior managers and all members of the University community of their obligations under data protection law,
- Promoting a culture of data protection, e.g. through training and awareness activities,
- Reviewing and recommending policies, procedures, standards, and controls to maintain and demonstrate compliance with data protection law and embed privacy by design and default across the University,
- Advising on data protection impact assessment and monitoring its performance,
- Monitoring and reporting on compliance to the University Executive, the Audit and Risk Committee and other relevant committees and boards,
- Maintaining Records of Processing Activities,
- Providing a point of contact for data subjects regarding all issues related to their rights under data protection law,
- Investigating personal data breaches, recommending actions to reduce their impact and likelihood of recurrence,
- Acting as the contact point for and cooperating with the UK Information Commissioner's Office and other applicable supervisory authorities on issues relating to processing.

5.6 All Chief Operating Officers, Chief Executives of Global Research Institutes, Heads of Schools, Global Directors and Heads of Professional Services are responsible for implementing the policy within their business areas, and for adherence by their staff. This includes:

- Assigning generic and specific responsibilities for data protection management,
- Managing access rights for information assets and systems to ensure that staff, contractors and agents have access only to such personal data as necessary for them to fulfil their duties,
- Ensuring that all staff in their areas of responsibility undertake relevant training provided by the University and are aware of their responsibilities for data protection,
- Ensuring that staff responsible for any locally managed IT services liaise with University Information Services staff to put in place equivalent IT security controls,

- Assisting the Data Protection Officer in maintaining accurate and up to date records of data processing activities.

5.7 **The Global Director of Information Services** is responsible for ensuring that centrally managed IT systems and services embed privacy by design and default and for promoting good practice in IT security among staff.

5.8 **The Global Director of Human Resources** is responsible for maintaining relevant human resources policies and procedures, to support compliance with data protection law.

5.9 **The Global Academic Registrar** is responsible for maintaining relevant student administration policies and procedures and for oversight of the management of student records and associated personal data across the University in compliance with data protection law.

5.10 **The Head of Assurance Services** is responsible for ensuring that data protection and wider Information Security controls are integrated within project management, risk, business continuity management and audit programmes and for liaising with insurers to ensure that the ISMS meets insurance requirements.

5.11 **The Head of Procurement Services** is responsible for ensuring that supply chain due diligence and procurement processes embed information risk and data protection impact assessment and privacy by design.

5.12 **The Head of Safeguarding Services** is responsible for ensuring that controls to manage the physical security of the University take account of relevant data protection risks and are integrated into the ISMS.

5.13 **The Global Information Governance and Data Protection Committee** is responsible for reviewing the effectiveness of data protection policies and procedures as part of its wider oversight of information security management, as set out in the Information Security Policy Framework.

6. MONITORING AND EVALUATION

6.1 The Data Protection Officer will monitor new and on-going data protection risks and update the relevant University strategic risk register, reporting this promptly as required to the Global Director of Governance and Legal Services and the Head of Assurance Services. The Data Protection Officer will liaise with the Global Director of Information Services and the Head of Assurance Services to ensure that IT security risks related to data protection are captured on the register and that Schools, Institutes and Professional Service record data protection and information security risks on their local registers and escalate these as necessary to the Head of Assurance Services.

6.1 The Data Protection Officer will make regular reports to the University Executive and other Committees and Boards on data protection compliance.

POLICY

6.2 As part of the University's internal audit programme, the Audit and Risk Committee will instruct the University's Internal Auditors to audit the management of privacy and data protection risks and compliance with relevant controls, as required.

7. IMPLEMENTATION

This policy is implemented through the development, implementation, monitoring and review of the component parts of the University Information Security Management System.

These will require:

- The Data Protection Officer to liaise with Heads of Schools, Directors of Professional Services and their managers to review and update information risk assessments and records of processing activities and take necessary actions to identify and protect personal data and systems used to process the data;
- Coordination of effort between relevant Directors, Division Heads and professional specialists to integrate IT, physical security, people, information management, risk management and business continuity to deliver effective and proportionate information security controls;
- Review and refresh of all relevant policies and procedures;
- Generic and role specific training and awareness;
- Embedding data protection by design and default and related information governance requirements into procurement, project management and the implementation of software applications or process enhancements;
- Information security incident management policies and procedures;
- Business continuity management;
- Monitoring compliance and reviewing controls to meet business needs.

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1. University Policies and procedures

This policy forms part of an interconnected set of University Information Governance and IT Policies and procedures which are published on the University website at https://www.hw.ac.uk/about/policies.htm.

University privacy notices and further information about how data subjects can use their rights under data protection law are published at

POLICY

https://www.hw.ac.uk/uk/services/information-governance/protect/privacy-and-your-data-rights.htm

Managers of staff whose roles do not require University IT access are responsible for briefing their staff on their responsibilities in relation to all policies that affect their work.

8.2 Legal Requirements and external standards

Effective data protection and information governance controls are essential for compliance with U.K. and Scottish law and other relevant legislation in all jurisdictions in which the University operates:

UK GDPR
UK Data Protection Act 2018
The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
The EU GDPR, Regulation (EU) 2016/679

All current UK Legislation is published at http://www.legislation.gov.uk/

Laws of Malaysia: Act 709: Personal Data Protection Act 2010

Heriot-Watt University is a Scottish Public Authority under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004. These laws provide public rights of access to information held by the University, subject to the exemptions set out under this legislation. These exemptions include personal data that a data subject is entitled to request under the UK GDPR and DPA 2018 and information which, if disclosed, would breach any of the data protection principles. The UK GDPR (Article 2 1A) and DPA 2018 (Section 24) provide limited and conditional rights for data subjects to access manual unstructured data held by FOI Public Authorities, including the University.

UK Information Commissioner's Office (ICO)
Guidance on the UK GDPR
Privacy and Electronic Communications Regulations
Age Appropriate Design Code
Data Sharing Code
Data Protection Guidance

Joint Information Systems Committee (Jisc)
Guidance on Data Protection for universities and colleges

9. DEFINITIONS

The University	All references to the University in this policy mean the Heriot-Watt University Group.
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, biometric or genetic data, the spoken word, data stored on computers or

POLICY

	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 an identified or identifiable living person. An identifiable living person is someone who can be identified directly or indirectly from an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Although the GDPR and the Data Protection Act 2018 apply only to living people, the scope of this policy also includes information about deceased individuals. 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.
Special categories of Personal Data	Special categories of Personal Data (formerly known as sensitive personal data) (as defined in Articles 9 and 10 of the GDPR) are personal data relating to an identifiable person's: a) racial or ethnic origin, b) political opinions, c) religious or philosophical beliefs, d) membership of a trade union, e) physical or mental health or condition, f) sexual life or sexual orientation, g) proven or alleged offences, including any legal proceedings and their outcome, h) genetic or biometric data when processed to identify that individual. In addition, the University definition of High-Risk Confidential Information includes the following personal data: IT user passwords, Any other information that would cause significant damage or distress to an individual it was disclosed without their consent, such as bank account and financial information, marks or grades.
Data protection law	Relevant privacy legislation includes but is not confined to European Union General Data Protection Regulation 2016/679 (GDPR), the UK GDPR and UK Data Protection Act, 2018, UK

POLICY

	Privacy and Electronic Communications Regulations, the Malaysia Personal Data Protection Act, 2010, and equivalent legislation, in other jurisdictions in which the University operates.
Data Controller	An organisation which determines the purposes for which personal data is processed and is legally accountable for the personal data that it collects and uses or contracts with others to process on its behalf.
Data Processor	In relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Subject	A living person whose personal data is held by the University or any other organisation.
Natural person	A living person, not a “legal person” i.e. a company or other legal entity.
Processing	Any operation performed on personal data, such as collecting, creating, recording, structuring, organising, storing, retrieving, accessing, using, seeing, sharing, communicating, disclosing, altering, adapting, updating, combining, erasing, destroying or deleting personal data, or restricting access or changes to personal data or preventing destruction of the data.
Confidential information	The definition of confidential information can be summarised as: ▪ Any personal information that would cause damage or distress to individuals if disclosed without their consent, ▪ Any other Information that would prejudice the University's or another party’s interests if it were disclosed without authorisation. More details can be found in our information security classification scheme.
Information Security Management System (ISMS)	“That part of the overall management system based on a business risk approach to establish, implement operate, monitor, review, maintain and improve information security. The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.” BS ISO/IEC 27001: Information Security.

POLICY

Anonymisation	Irreversible removal of personal identifiers from information so that the data subject is no longer identifiable. Anonymised information therefore no longer falls within the definition of personal data.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person. Pseudonymised data is therefore re-identifiable and falls within the definition of personal data.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning their performance at work or studies, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Restriction of processing	The marking of stored personal data with the aim of limiting their processing in the future.
Records of Processing Activities	Detailed records of the personal data processing activities that a Data Controller or Processor is required to maintain and make available under the accountability principle of the GDPR.
Substantial public interest conditions	The UK Data Protection Act 2018 Schedule 1 defines conditions for processing special categories of personal data or data about criminal offences. Those that potentially apply in the University context are set out in Appendices 2 and 3.
Supervisory authority	An independent public authority established by the UK or another state to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of non-compliance. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

10. FURTHER HELP AND ADVICE

For further information and advice about this policy and any aspect of information security contact:
Information Governance
Telephone: +44 (0)131 451 3274/3216/3219
Email: dataprotection@hw.ac.uk

POLICY

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V8.4 11/11/2021	16 December 2021. Update of policy previously approved on 23 February 2018.	Court; on the recommendation of the Audit and Risk Committee, University Executive, Global Operations Executive and Global Information Governance and Data Protection Committee.	Updated to take account of impact of Brexit on GDPR, consequential changes to the UK Data Protection Act, the ICO Age Appropriate Design Code and other legal developments relating to the University's international risk environment. Version 8.4 takes account of feedback from the Global Operations Executive, the Joint HR and Trade Union Policy Working Group and the Audit and Risk Committee.

POLICY

Appendix 1

GDPR Conditions for processing personal data (GDPR Article 6 conditions in brackets)
The UK Data Protection Act 2018 allows for the introduction of more specific provisions in relation to Articles 6(1)(c) and (e)
The data subject has given consent to the processing of his or her personal data for one or more specific purposes. (6(1)(a))
Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. (6(1)(b))
Processing is necessary for compliance with a legal obligation to which the controller is subject. ((6(1)(c)) This may apply where the University has a statutory obligation to disclose personal information to a government agency.
Processing is necessary in order to protect the vital interests of the data subject or of another natural person. (6(1)(d)) This condition only applies in “life or death” situations, such as where a hospital’s A&E department need to contact the GP or medical doctor of an unconscious individual they are treating after a serious road accident.
Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (6(1)(e)). This condition applies to public authorities only. As a Scottish public authority under the Freedom of Information (Scotland) Act 2002, the University is also a public authority under the GPDR and the DPA 2018. This condition applies to academic and other activities that the University carries out under the powers and obligations defined in its Charter and Statutes.
Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. Except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (6(1)(f)) This condition does not apply to processing carried out by the University in the performance of its tasks under powers defined in the Charter and Statutes. The University may be able to rely on legitimate interests under other limited circumstances.

POLICY

Appendix 2

GDPR Conditions for processing special categories of personal data (GDPR Article 9 conditions in brackets) Data controllers must satisfy a lawful condition of processing personal data under Article 6 of the GDPR as well as one under Article 9 to process these categories of data.
The UK Data Protection Act 2018 introduces more specific provisions. These **substantial public interest conditions** are subject to appropriate safeguards set out in DPA 2018 for provision of transparent policy governing the processing, records retention policy and records of processing activities. (DPA 2018 Schedule 1)
The data subject has given explicit consent to the processing. (9(2)(a))
The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law. (9(2)(b)) DPA 2018 substantial public interest safeguards apply.
The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent. (9(2)(c))
The processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and does not involve disclosing personal data to a third party, unless the data subject consents. Extra limitations apply to this condition. (9(2)(d))
The data subject has deliberately made the information public. (9(2)(e))
The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (9(2)(f))
Processing is necessary for reasons of substantial public interest, on the basis of EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (9(2)(g))
The processing is necessary for health or social care purposes of— (a) preventive or occupational medicine, (b) the assessment of the working capacity of an employee, (c) medical diagnosis, (d) the provision of health care or treatment, (e) the provision of social care, or (f) the management of health care systems or services or social care systems or services, On the basis of EU or UK law and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality. (9(2)(h)) (DPA 2018 Schedule 1 1 2)

Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or UK law (9(2)(i)) and is carried out— (i) by or under the responsibility of a health professional, or (ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law. (DPA 2018 Schedule 1 1 2)
Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the safeguards set out in GDPR Article 89(1) based on EU or UK law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (9(2)(j))
Equality of opportunity or treatment The processing is in the substantial public interest and necessary for monitoring and promoting of equality of opportunity between: • people of different racial or ethnic origins, • people holding different religious or philosophical beliefs, • people with different states of physical or mental health, • people of different sexual orientation. As long as the processing is NOT: • carried out for the purposes of measures or decisions with respect to a particular data subject, • carried out without that data subject's consent, • likely to cause substantial damage or substantial distress to an individual. (DPA 2018 Schedule 1 Part 2 (7))
Preventing or detecting unlawful acts The processing: 1 a) is necessary for the purposes of the prevention or detection of an unlawful act, (b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and (c) is necessary for reasons of substantial public interest. (2) In this paragraph, "act" includes a failure to act. (DPA 2018 Schedule 1 Part 2 (8))
Protecting the public against dishonesty etc. The processing: (a) is necessary for the exercise of a protective function, (b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and

(c) is necessary for reasons of substantial public interest.
(2) In this paragraph, “protective function” means a function which is intended to protect members of the public against:
(a) dishonesty, malpractice or other seriously improper conduct,
(b) unfitness or incompetence,
(c) mismanagement in the administration of a body or association, or
(d) failures in services provided by a body or association.

(DPA 2018 Schedule 1 Part 2 (9)). DPA 2018 Schedule 1 Part 2: (10) also makes provision for disclosures by journalists in the public interest for the same purposes as set out in 9.

Counselling etc.

The processing:
1 (a) is necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially,
(b) is carried out without the consent of the data subject for a reason listed in sub-paragraph (2), and
(c) is necessary for reasons of substantial public interest.
(2) The reasons mentioned in sub-paragraph (1)(b) are—
(a) in the circumstances, consent to the processing cannot be given by the data subject,
(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing,
(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the service mentioned in sub-paragraph (1)(a).
(DPA 2018 Schedule 1 Part 2 (13))

POLICY

Appendix 3

GDPR Conditions for processing personal data about criminal offences (GDPR Article 10 conditions in brackets) Data controllers must satisfy a lawful condition of processing personal data under Article 6 of the GDPR as well as one under Article 9 to process these categories of data.
The UK Data Protection Act 2018 introduces more specific provisions. These **substantial public interest conditions** are subject to appropriate safeguards set out in DPA 2018 for provision of transparent policy governing the processing, records retention policy and records of processing activities. (DPA 2018 Schedule 1.

Where we are relying on substantial public interest to process special categories of personal data or criminal offences personal data we must have an appropriate policy document in place specifying • Which condition we rely on • How we comply with the data protection principles • How long we retain the data We must also complete a Data Protection Impact Assessment and maintain accurate records of processing activities.

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by UK law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. (10)
Employment, social security and social protection 1(1)This condition is met if— (a) the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection, and (b) when the processing is carried out, the controller has an appropriate policy document in place (DPA 2018 Schedule 1 Part 1(1)
Research etc. 4 This condition is met if the processing— (a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes,

(b) is carried out in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19), and (c) is in the public interest. (DPA 2018 Schedule 1 Part 1(4)
Preventing or detecting unlawful acts 10(1) This condition is met if the processing— (a) is necessary for the purposes of the prevention or detection of an unlawful act, (b) must be carried out without the consent of the data subject so as not to prejudice those purposes, and (c) is necessary for reasons of substantial public interest. (2) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule). (3) In this paragraph— “act” includes a failure to act; “competent authority” has the same meaning as in Part 3 of this Act (see section 30). DPA 2 018 Schedule 1 Part 2 10 (1)
Protecting the public against dishonesty etc. 11(1) This condition is met if the processing— (a) is necessary for the exercise of a protective function, (b) must be carried out without the consent of the data subject so as not to prejudice the exercise of that function, and (c) is necessary for reasons of substantial public interest. (2) In this paragraph, “protective function” means a function which is intended to protect members of the public against— (a) dishonesty, malpractice or other seriously improper conduct, (b) unfitness or incompetence, (c) mismanagement in the administration of a body or association, or (d) failures in services provided by a body or association. DPA 2018 Schedule 1 Part 2: 11
Regulatory requirements relating to unlawful acts and dishonesty etc. 12(1) This condition is met if— (a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has— (i) committed an unlawful act, or (ii) been involved in dishonesty, malpractice or other seriously improper conduct, (b)in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and

(c) the processing is necessary for reasons of substantial public interest.
(2) In this paragraph—
"act" includes a failure to act;
"regulatory requirement" means—
(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or
(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.

DPA 2018 Schedule 1 Part 2: 12

Preventing fraud

14(1) This condition is met if the processing—
(a) is necessary for the purposes of preventing fraud or a particular kind of fraud, and
(b) consists of—
(i) the disclosure of personal data by a person as a member of an anti-fraud organisation,
(ii) the disclosure of personal data in accordance with arrangements made by an anti-fraud organisation, or
(iii) the processing of personal data disclosed as described in sub-paragraph (i) or (ii).
(2) In this paragraph, "anti-fraud organisation" has the same meaning as in section 68 of the Serious Crime Act 2007.

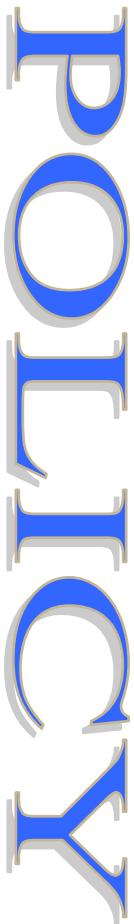
DPA 2018 Schedule 1 Part 2: 14

Safeguarding of children and of individuals at risk

18(1) This condition is met if—
(a) the processing is necessary for the purposes of—
(i) protecting an individual from neglect or physical, mental or emotional harm, or
(ii) protecting the physical, mental or emotional well-being of an individual,
(b) the individual is—
(i) aged under 18, or
(ii) aged 18 or over and at risk,
(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and
(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—
(a) in the circumstances, consent to the processing cannot be given by the data subject;
(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;
(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).
(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—
(a) has needs for care and support,
(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it. (4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual. DPA 2018 Schedule 1 Part 2: 18
Consent 29 This condition is met if the data subject has given consent to the processing. DPA 2018 Schedule 1 Part 3: 29
Protecting individual's vital interests 30 This condition is met if— (a) the processing is necessary to protect the vital interests of an individual, and (b) the data subject is physically or legally incapable of giving consent. DPA 2018 Schedule 1 Part 3: 30
Personal data in the public domain 32 This condition is met if the processing relates to personal data which is manifestly made public by the data subject. DPA 2018 Schedule 1 Part 3: 32
Legal claims 33 This condition is met if the processing— (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights. DPA 2018 Schedule 1 Part 3: 33



Appendix 4

GDPR Conditions for processing personal data **by consent** (Article 7 and Recital 32)
Where processing is based on consent, the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.
Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This can include opting in to share data using a social media application.
Silence, pre-ticked boxes or inactivity should not therefore constitute consent.
If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
Consent will not be freely given if the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Appendix 5

GDPR Conditions for processing personal data **by consent where the data subject is a child** (GDPR Articles 8 and 17)
In relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. The GDPR makes provision for a lower age of 13 where domestic law allows for this. Under the DPA 2018, in Scotland a person aged 12 or over is presumed to have capacity to give consent to processing and to exercise his or her rights. In the rest of the UK the presumed age is 13. In other jurisdictions higher age thresholds may apply. Under relevant laws in Dubai and Malaysia, a child's parent or guardian will exercise all data subject rights on behalf of the child until the child reaches the age of 18. Where a child is below the relevant age thresholds, the controller shall make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. The GDPR does not affect general contract law such as the rules on the validity, formation or effect of a contract in relation to a child. Information society services are online services such as social media platforms. It should be noted that the UK Information Commissioner's Office statutory Age Appropriate Design Code applies to online services that are likely to be accessed by any child under the age of 18, regardless of whether the service is aimed at children. Where a data subject asks for personal data processed via social media to be erased, the Data Controller must inform other recipients of the data subject's request and seek to take down online links to the data.

POLICY