HSU HEALTH SCIENCES UNIVERSITY

Data Protection Policy

Contents

1. Introduction

1.1 Health Sciences University (HSU) is committed to data protection by default and by design and supports the data protection rights of all those with whom it works, including, but not limited to its staff, students, visitors, alumni and research participants.

1.2 Health Sciences University acknowledges that handling personal data properly and in compliance with data protection legislation enhances trust, is the right thing to do and protects HSU's relationship with all its stakeholders.

1.3 This Data Protection Policy:

1.3.1 Regulates the way in which HSU obtains, uses, holds, transfers and otherwise processes personal data about individuals and ensures that all HSU staff, students, visitors and third parties who process personal data ("Users") comply with the rules for protecting personal data, this includes the use of Artificial Intelligence (AI).;

1.3.2 Describes individuals' rights in relation to their personal data processed by HSU. In the context of this Data Protection Policy, staff includes; prospective, current and former employees, contractors, agency workers, consultants, volunteers, students, apprentices, and those undertaking work experience at HSU.

1.3.3 It is important that affected individuals carefully read this Data Protection Policy and any other data protection policy provided to them on specific occasions when HSU is collecting or processing the individual's personal data to ensure that individuals are fully aware of how and why HSU are using the individual's personal data. This policy supplements other notices and privacy policies and is not intended to override them.

2. Definitions

2.1. The UK General Data Protection Regulation (GDPR) governs the processing of personal data. The following definitions are used:

- **Personal Data** is data which can identify living individuals. As well as images, names and contact details it can also include numerical or statistical information from which an individual's identity can be derived.
- **Special Category Data** are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- A **Data Subject** is the individual who is the subject of personal data.
- A **Data Controller** determines the purposes for which personal data are processed. The controller is ultimately responsible for the personal data, whether they pass the data to a data processor or not. This includes the responsibilities of responding to Subject Access Requests and complaints from data subjects.
- A **Data Processor** is any individual or organisation who processes personal data on behalf of – and according to the purposes defined by – the data controller.
- **Artificial Intelligence** we use the umbrella term 'AI' because it has become a standard industry term for a range of technologies. One prominent area of AI is 'machine learning' (ML), which is the use of computational techniques to create (often complex) statistical models using (typically) large quantities of data. Those models can be used to make classifications or predictions about new data points. While not all AI involves ML, most of the recent interest in AI is driven by ML in some way, whether in image recognition, speech-to-text, or classifying credit risk.

3. Personal Data

3.1 Personal data is defined in Article 4 of the UK General Data Protection Regulation 2016/679 ("GDPR") as any information (for example, a person's name) or combination of information about a living person which allows that living person to be identified from that information (for example a first name and an address). Personal data can also include an online identifier or one or more factors specific to the physiological, genetic, mental, economic, cultural or social identity of an individual. Examples of Personal Data which may be used by HSU in its day-to-day business include (but are not limited to):

- names, addresses (e-mail and postal addresses);
- telephone numbers and other contact details;
- CVs;
- Appraisals;
- payroll and salary information; and
- health information and financial information

3.2. The definition of personal data also includes opinions, appraisals or intent regarding individuals (e.g. employees, job applicants, students, personal contacts at suppliers and individual members of the public).

4. Scope of the Policy

4.1 The laws governing how Health Sciences University can use personal data (including UK GDPR and the Data Protection Act 2018) apply whether the personal data is stored electronically (for example, in e-mails, on IT systems, as part of a database or in an Eletronic file , AI system) or in structured manual records (for example, in paper files or filing cabinets).

4.2 This Data Protection Policy:

- applies to any and all HSU users;
- covers the processing of all personal information whose use is controlled by HSU; and
- covers all personal information handled, stored, processed or shared by HSU whether organised and stored in physical or IT based record systems.

5. Status

5.1 Health Sciences University is a Data Controller and also a Data Processor for certain activities.

5.2 Health Sciences University must:

- meet its legal obligations as a data controller or processor, including data protection by design and default;
- where necessary, conduct data protection impact assessments;
- maintain records of processing activities;
- have in place measures to ensure the security of processing;
- have a clear procedure for the handling of data breaches; and
- have appointed a Data Protection Officer.

6. Purpose

6.1 The purpose of this Data Protection Policy is to set out the accountability and responsibilities of Health Sciences University and Users in complying fully with the provisions of the General Data Protection Regulation ("the GDPR") and the Data Protection Act 2018 ("the DPA") and to define;

- What personal data HSU collect about individuals;
- How HSU collects personal data;
- How HSU uses personal data;
- Data subject's rights;
- Making a complaint;
- How and why HSU shares personal data;
- Transferring personal data overseas;
- How long HSU holds personal data;
- Links to other websites; and
- Changes to the Data Protection Policy

6.1. The Data Protection Act 2018 and the GDPR govern the collection, holding, processing and retention of all personal data relating to living individuals. Its purpose being to ensure that those organisations and individuals, who collect, store and use that data do not abuse it, and process the data in accordance with the following data protection principles that personal data shall:

i. be processed lawfully, fairly and in a transparent manner;
ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
iii. be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
iv. be accurate and kept up to date;
v. not be kept for longer than is necessary for those purposes;
vi. be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

6.2. The University and its staff, students and contractors that process or use personal data on behalf of the University must comply with these principles and ensure that they are followed at all times.

7. Data Processing Activity

7.1 The University collects and processes Personal Data on its employees, students, applicants and former employees, for a multitude of purposes, including:

- Maintenance of the Student record;
- Recruitment;
- Employee performance management and professional development;
- Payroll;
- Business and market development;
- Building and managing external relationships;
- Research and development;
- Planning and delivering of education and training;
- Staff and student support and facilities management;

- Health, safety and security; and
- Other purposes required by law or regulation.

7.2 When we collect, record, store, use, share or erase Personal Data for any of these purposes, this is called processing, including if it is carried out by automated means. If you read, amend, copy, print, delete or send Personal Data, this is a type of "processing" and is subject to the guidelines set out in this Policy.

8. Data Security

8.1 As a data controller, Health Sciences University has a responsibility under Article 24 of the GDPR, to ensure that there are appropriate technical and organisational measures in place to ensure that all data processing is performed in accordance with data protection law. The University must keep all Personal Data (including Special Category Data) secure. This means that the Personal Data must be protected against being accessed by other organisations, systems such as AI (when not intended for use) or individuals (for example, via hacking), from being corrupted or being lost or stolen. The Personal Data must also be protected so the wrong people or systems such as AI (when not intended for use) cannot read or use the details. All staff must comply with the University's security procedures whenever they handle Personal Data. The University requires staff to keep data secure and to comply with the University's Computer Acceptable Use Policy.

8.2 All staff, students, contractors and partnership organisations must ensure that any personal information, which they hold, is kept securely and that they take appropriate security precautions by seeking to ensure the following:

- Source documents are kept in a lockable cabinet or drawer or room;
- Computerised data is password protected or stored in a secure area with restricted access permissions to those who require access;
- Authorised sharing of personal data must be transferred securely via Encrypted or password protected means;
- Personal information is not disclosed orally or in writing, or in any other way, intentionally or otherwise to any unauthorised personnel;
- Data kept on discs or data storage devices are stored securely and encrypted;
- Ensure individual passwords are kept confidential and are not disclosed to other personnel enabling log-in under another individual's personal username and password;
- Logged on PCs are not left unattended where data is visible on screen to unauthorised personnel;
- Screensavers are used at all times;
- Paper-based records must never be left where unauthorised personnel can read or gain access to them.

8.3 If a member of staff works away from the University's premises, they must comply with the additional procedures and guidelines issued by the University for home working and offsite working, as this presents a potentially greater risk of loss, theft or damage to personal data. You must read these procedures and guidelines before processing any personal data away from the University premises.

9. Lawfulness of Processing Data

9.1 One of the main data protection obligations requires the University (and its employees) to process Personal data lawfully, fairly and in a transparent manner (this includes when using AI). This means under Article 6 that the University must comply with at least one of the following conditions when processing Personal Data:

- the individual to whom the Personal Data relates has consented to the processing;
- the processing is necessary for the performance of a contract between the University and the individual;
- the processing is necessary to comply with a legal obligation placed on the University;
- the processing is necessary to the legitimate interests of the University or a third party affiliate;
- the processing is necessary to protect a vital interest of the individual or another person;
- the 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 University.

9.2 The individual's consent to processing Personal Data should only be relied upon where there is no other lawful reason to process data.

9.3 If in any doubt about the lawful, fair and transparent use of Personal Data, you should consult the appropriate Privacy Notice and contact the Data Protection Officer.

10. Special Category and Criminal Convictions Data

10.1 Special Category Data (previously known as sensitive personal data) is Personal Data about a person's race or ethnicity, their health, their sex life or sexual orientation, their religious or philosophical beliefs, their political views or trade union membership, their physical or mental health or condition, genetic or biometric data.

10.2 In some cases, the University is required to process special category data and data about actual or alleged criminal convictions and any associated proceedings. This type of personal data is afforded additional protection under data protection legislation (the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)) and we must only process it if certain conditions can be met.

10.3 The University processes special data and data about criminal convictions in reliance on the following conditions from Schedule 1 DPA.

10.4 <u>Employment, social security and social protection</u>
The University processes a variety of information about prospective, current and previous employees for employment purposes, including data about health and criminal convictions and associated proceedings. It is not appropriate to obtain consent for such processing due to the nature of the employer-employee relationship and because consent cannot be freely given or withdrawn; therefore the University relies on this condition for much of this processing. Personal data processed for employment purposes is treated confidentially and maintained by HR as part of applicant and employee personal files.

10.5 <u>Statutory and government purposes</u>
The University is legally required to provide some special category data about staff and students to external organisations for statutory returns and reporting, such as the data we provide to the Higher Education Statistics Agency (HESA). Only the minimum amount of data necessary to fulfil this requirement is provided and all data is shared securely. We also rely on this condition to process data about students' criminal convictions.

10.6 Preventing or detecting unlawful acts

We rely on this condition to process data about applicants' and students' criminal convictions, in certain circumstances, to enable us to manage any potential risks to the University community. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements. We may also rely on this condition to process information about employees' criminal convictions, if appropriate.

10.7 Protecting the public against dishonesty etc.

The University runs courses which lead to entry into a regulated profession. We may disclose special category data or data about criminal convictions to those who regulate such professions so that those regulators can exercise their functions appropriately by ensuring practitioners are fit and proper. There is a substantial public interest in enabling regulators to ensure that only those who are fit to practice a particular profession or occupation are able to do so.

10.8 Regulatory requirements relating to unlawful acts and dishonesty etc.

Where it is not appropriate to rely on consent, the University relies on this condition when it processes special category data and criminal convictions data about Members of its Board of Governors (the Company Directors/Charity Trustees)(as well as some employees) to ensure they are fit and proper persons to fulfil the role. To enable us to register as a higher education provider with the Office for Students, we must be able to demonstrate that the University has appropriate management arrangements in place which do not present a risk to students or to public funds, such as dishonesty.

11. Age Verification Required for Children and Process for Gaining Consent from Parent/Guardian

11.1. Children have the same rights as adults over their personal data which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility must exercise the child's data protection rights on their behalf.

11.2. Children need particular protection when we are collecting and processing their personal data because they may be less aware of the risk involved.

11.3. A child's personal data merits particular protection under the GDPR.

11.4. We rely on consent as our lawful basis for processing personal data when offering a service directly to children, in the UK only children aged 13 or over are able to provide their own consent. Therefore we must verify that anyone giving their own consent in these circumstances is old enough to do so. For children under this age, we will get consent from whoever holds parental responsibility for them. We must also make reasonable efforts to verify that the person giving consent does, in fact, hold parental responsibility for the child.

12. Privacy Notices

12.1 When the University collects Personal Data from people then it must at the time of collection, provide them with certain information that is included in our Privacy Notices.

12.2 In accordance with Article 5 of the GDPR, any processing of Personal Data must be undertaken lawfully, in a fair and transparent manner. In accordance with Article 13, the University must provide the data subject with a Privacy Notice and provide certain

information within that notice including:

- Name and contact details of the person collecting the Personal Data and the University DPO,
- The purpose and legal basis for processing the data,
- Any disclosure or sharing with third parties,
- Whether it will be transferred out of the country
- Whether AI may be involved in the processing of personal data and if it is, how it will use the data and ensure safe, and fair use of the data including decision making.

12.3 For this purpose the University has privacy notices for students, staff, research participants, external examiners and patients which are available from https://www.hsu.ac.uk/privacy-policy/

12.4 You should therefore check whether there is an applicable notice which covers the processing you intend to carry out for the University. In cases where there is not an appropriate notice, you should contact the DPO before any processing commences. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

12.5 The University must also provide the individual with information on the period for which the Personal Data will be stored, the individual's rights on rectification, erasure and data portability, whether automated decision making or profiling will be carried out and the right to withdraw consent to processing if that is relied upon as the lawful basis for processing.

13. Processing Relevant Data and Keeping It Accurate

13.1 Personal Data (including any Special Category Data) must be appropriate to, and sufficient for, the relevant purpose(s) it is collected for, and not excessive for that purpose(s). Only the data which is necessary for the task can be processed. For example, if you never telephone someone at home, you do not need to record their home telephone number.

13.2 In addition, it is vital that care is taken to record and input Personal Data accurately. This is very important. There can be serious risks for the University if Personal Data is incorrect. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date.

14. Accuracy of Data

14.1 Staff are responsible for:

i. ensuring that any information they provide to the University relating to their employment is accurate and up to date;
ii. informing the University of any information changes, e.g. change of address, vehicle registration number or bank account details;
iii. checking the information that the University may send out from time to time giving details of information kept and processed about staff;

14.2 Students must also ensure that all data provided to the University is accurate and up- to-date by either notifying the Registry team at registry@aecc.ac.uk or updating their student details online during annual registration (an annual process for all HSU students) or by emailing Registry at registry@aecc.ac.uk.

14.3 The University cannot be held responsible for any errors unless the member of staff or student has informed the University about them.

15. Data Retention

15.1 The University cannot keep or retain Personal Data forever. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws). Other records must only be kept while in current use and for a reasonable period afterwards. In order to comply with law, the University has a Records Retention Policy.

15.2 As a general rule, when Personal Data is no longer needed by the University for the purposes for which it was collected, this Personal Data should be securely destroyed as soon as practicable.

16. Data Subjects' Rights

16.1 Individuals have certain rights in relation to their Personal Data:

- the right to access Personal Data held about themselves;
- the right to prevent processing of Personal Data for direct marketing purposes;
- the right to have Personal Data rectified if it is inaccurate;
- the right to have their Personal Data erased (the 'right to be forgotten');
- the right to restrict processing in certain circumstances;
- the right to data portability in certain circumstances;
- the right to compensation for any damage/distress suffered; and
- the right to be informed of automated decision making about them and the right to object to such processing and to not be subject to automated decision making which produced legal effects concerning the individual.

16.2 If you should receive an enquiry about any of the above rights that you are unsure about, then you should seek advice from the Data Protection Officer.

16.3 Individuals are allowed to withdraw their consent to the University's use of their Personal Data at any time. However, the University will only be relying on consent to process Personal Data in very limited circumstances. Other lawful reasons for processing will be relied upon where possible. If an individual contacts you to withdraw their consent, inform the Data Protection Officer promptly.

17. Subject Access Requests (SARs)

17.1 Under Articles 12 – 15 of GDPR individuals can ask for copies of the Personal Data the University holds about them and other details about how the University uses their Personal Data including any processing carried out with AI tools. If you receive such an access request, there are special legal rules which must be followed as part of this process. Therefore, please inform the Data Protection Officer immediately and follow their instructions. You must not deal with such requests in isolation.

17.2 A data subject can request from the University to:

- Confirm whether or not their Personal Data is being processed, the purpose of the processing and categories of data processed,
- Have access to that data (a copy is normally provided)
- The data subject may also request:
- The recipients or categories of recipient to whom the Personal Data have or will be disclosed, in particular recipients in third countries or international organisations,

- Where possible the envisaged period for which the Personal Data will be stored, or the criteria used to determine that period,
- The existence of the right to request rectification or erasure of Personal Data or restriction from processing of Personal Data concerning the data subject, or to object to such processing,
- The right to lodge a complaint with the ICO,
- Where the data was not collected from the Data subject, any available information as to the source,
- Where Personal Data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer,
- Information on the existence of any automated decision making, including profiling;
- To be provided with copies of the Personal Data held about him or her.

17.3 The University's Subject Access Request Policy & Procedure is available on the website here: https://www.hsu.ac.uk/subject-access-requests/

18. Data Loss or Security Breach Procedure

18.1 There are potentially significant repercussions for the University and the individuals affected arising from a data loss or security breach. Where this occurs or you suspect it may have occurred you must follow the guidance provided in the University's Data Breach Procedure:

- It is important that this is done immediately, as it may be possible to reduce the impact of the breach by remote deletion, removal or other means.
- Follow their guidance on dealing with the security breach and keep the DPO up to date with any further information about it that you become aware of;
- Do not approach any individual data subjects, suppliers, regulators or make any public announcements about the security breach incident without the prior agreement of the Data Protection Officer.

19. Disclosure of Data

19.1 Any disclosure of Personal Data is a form of processing. That means that the rules described above concerning fair and lawful use have to be satisfied.

19.2 You should exercise caution and ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.

19.3 All requests to disclose personal data held on another individual to any third party must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

20. Disposal of Data

20.1. The destruction of personal data is of itself "processing" and must be carried out in accordance with the data protection principles.

20.2. Where you are disposing of personal data, you should ensure:

- that it is destroyed permanently and securely;
- it does not remain in your inbox, deleted items folder or recover deleted items

folder; and

- that hard copies of personal information are confidentially shredded or placed in confidential waste bins and not disposed of in a wastepaper basket /recycle bin.

21. Transfer of Data to Third Countries or International Organisations

21.1. The GDPR contains special rules on whether Personal Data collected in the UK can be transferred to another country. Within the UK, there are restrictions on the transfer of Personal Data outside of the European Economic Area (such a transfer can happen, for example, where Personal Data is e-mailed outside the EEA). This is to make sure the Personal Data remains safe and the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

21.2. The fact that there will be transfers of Personal Data to other countries, especially to outside the EEA, should be clearly set out in the privacy notices described in the fair use section of this Policy above so that it is expected by the affected individuals

21.3. Articles 44 – 50 of the GDPR cover the law regarding the transfer of data outside the EEA. For more information on overseas transfers please contact the Data Protection Officer.

21.4. Do not transfer personal data to third parties outside the EEA or Norway, Iceland and Lichtenstein without the prior authorisation from our Data Protection Officer.

22. Management and Legal Responsibilities

22.1. If you are a line manager, you should ensure that you and your reportee's have completed any and all training that the University has advised is required for job roles and ensure that you and your reportee's are familiar with all relevant requirements regarding the processing of all personal data to which they have access in the course of their duties.

22.2. If you are in any doubt about what you may or may not do with personal data, you should seek advice from your line manager or the Data Protection Officer before taking any action.

23. Data Collection for Marketing Purposes

23.1. Where the University intends to collect the Personal Data of people and use it for marketing purposes and the person must give clear, informed and specific consent to show that they understand what they are being asked to consent to. This will normally be by a series of tick boxes allowing the person to select how they wish to be contacted. This is known as 'opting in'. Boxes which require a person to tick if they do not want to be contacted, known as 'opting out' are no longer allowed and must not be used. Pre-ticked boxes which rely on an individual removing the tick if they do not consent to be contacted are also no longer acceptable.

23.2. Forms collected recording a data subject's consent to be contacted for marketing purposes should be retained and stored for as long as the University is sending them any marketing information.

24. Marketing

24.1. An individual has the right to prevent his/her personal data being processed for direct

marketing. An individual can, at any time, give written notice to stop (or not begin) using their personal data for direct marketing. Any individual can exercise this right, and if the University receives a notice then it must comply within a reasonable period.

25. Data Protection Impact Assessments (DPIAs)

25.1. Data Protection Impact Assessments (or Privacy Impact Assessments as they are sometimes known) are a tool to help the University identify the most effective way to comply with our data protection obligations and to meet individuals' expectations of privacy. It is a process that will help the University to identify and reduce the privacy risks of a project or process.

25.2. The University's DPIA Procedure can be found on the University SharePoint.

25.3. DPIAs should be conducted at an early stage in a project to allow for the assessment to influence and if necessary change the project, taking full account of privacy issues. A DPIA involves the examination of all data information flows and minimising any risk associated with the collection, retention, use and destruction of the data. DPIA's also include an examination of the necessity and proportionality of any data collection process and should also examine privacy issues associated with the project. This may include issues such as who has access to data, the organisational and technical measures in place to provide data security, intrusion into people's lives and steps taken to minimise these issues. Consultation with stakeholders and those affected must also be taken into account.

25.4. Examples of projects that may benefit from a DPIA include:

- Installation of new or additional CCTV cameras or systems
- A new database to record staff or student data
- A project to identify students of a particular group or demographic which may initiate a course of action
- A new building project to provide student accommodation
- A new database to consolidate several existing databases containing student or staff data
- A new process that involves AI

25.5. Please note that under the GDPR, non-compliance with requirements to conduct a DPIA may lead to enforcement action by the ICO. These assessments are an essential part of documenting how the University complies with its responsibilities under the GDPR and the Data Protection Act 2018.

25.6. If there is any doubt about whether or not to undertake a DPIA, the Data Protection Officer should be consulted for advice.

26. Liability and Breach

26.1. You must immediately report to your Line Manager and/or the Data Protection Officer any actual or suspected data protection breaches or breaches to this policy.

26.2. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal where there are significant or deliberate breaches of this policy, such as accessing employee or customer personal data without authorisation or a legitimate reason to do so.

27. Training and Awareness

27.1 All staff will be required to complete regular data protection training to ensure:

- Understanding of Data Protection responsibilities
- Ability to recognise potential breaches
- Use correct reporting process

28. Data Protection Officer (DPO)

28.1. Please note that reference is made throughout this document to the Data Protection Officer, who can be contacted via email: dpo@aecc.ac.uk.

29. Complaints

29.1. Complaints regarding the University's processing of personal data should be addressed to dpo@aecc.ac.uk

Version:	6
Approved by:	WMG
Originator / Author	Data Protection Officer
Owner	Data Protection Officer
Reference source	HE Exemplars
Date approved	June 2025
Effective from	June 2025
Review date	June 2028
Target	Health Sciences University Staff
Policy location	SharePoint and University website
Equality analysis	This Policy has been developed with due regard to the University College's general equality duty and no direct impact has been identified.