| | |
|---|---|
| **Document Reference #** | IHRI-ADM-POL-008 |
| **Document Title** | Privacy Policy |
| **Owner** | IHRI Administration |
| **Version** | 1.2 |
| **Issue Date** | 18/08/2025 |
| **Next Review Date** | 18/08/2026 |

# INTRODUCTION

## PURPOSE

The International Health Research Institute of Birkirkara, Malta (the "Institute"; "we"; "us" or "our") is wholly committed to protecting the privacy and security of the personal information of its students, staff and visitors ("you").

This privacy policy (the "policy") describes how we collect and use information about students, staff and visitors per the Data Protection Act (Chapter 440 of the Laws of Malta), as may be amended from time to time, and the General Data Protection Regulation (EU) 2016/679).

The Institute is a "data controller". This means that we are responsible for deciding how we hold and use personal information (i.e. "personal data") about students, staff and visitors to our digital ecosystem.

Under applicable data protection legislation, we are required to inform you about this policy's information. The Institute requires a certain amount of personal data about you to administer your studies, organise and provide your education, and comply with its statutory obligations.

During our administrative and educational functions, we (the Institute) will process your data as a data controller (which may be held on paper, electronically, or in another medium).
We recognise the need to treat it appropriately and lawfully, following the Data Protection Act (Chapter 440 of the Laws of Malta), as may be amended from time to time, and the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR" or the "Regulations").

The purpose of this policy is to outline the basis for processing personal data, inform you about our handling and care of personal data, and notify you of our obligations to process data responsibly, your data protection rights as a data subject, and the legal protections in place for individuals.

This policy applies to staff, visitors, and current and former students (full-time, part-time, and alumni). It does not form part of the student agreement. We may update or amend this policy at any time. You must read this policy and any other privacy policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are aware of how and why we are using your data.

## SCOPE

This policy applies to all IHRI staff, students and visitors using our digital ecosystems.

## DEFINITIONS

| TERM OR ABBREVIATION | DEFINITION |
|---|---|
| IHRI | International Health Research Institute |
| DPA | Data Protection Act, Chapter 440 of the Laws of Malta |
| GDPR | General Data Protection Regulation (EU) 2016/679) |
| Data Controller | This means any entity or individual who determines the purposes for and how personal data is processed. For this policy, the data controller is IHRI |
| Consent Form | This policy refers to separate documents we provide you from time to time in which we ask for your explicit consent for any processing that is not for purposes in this policy. |
| Data subjects | This policy means living individuals about whom we collect and hold personal data. |
| Data processor | This means any entity or individual that processes data on our behalf and on our instructions (we being the data controller). |
| EEA | European Economic Area |
| Personal data | This means data relating to a living individual can be identified from the data (information) we hold or possess. This includes but is not limited to, your name and surname (including maiden name where applicable), address, date of birth, nationality, gender, civil status, tax status, identity card number & passport number, contact details (including mobile and home phone number and personal email address), photographic image, bank account details, emergency contact information as well as online identifiers. The term "personal information", where and when used in this policy, shall have the same meaning as personal data. |
| Processing | This means any activity that involves the use of personal data. It includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties. |
| Sensitive personal data, sensitive data or special categories of personal data | This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, or sexual life, or about the commission of or proceedings for any offence committed or alleged to have been committed by that person, the disposal of such |

| | |
|---|---|
| | proceedings, or the sentence of any court in such proceedings. This type of sensitive data can only be processed under strict conditions. |

## DATA PROTECTION PRINCIPLES

We will make every effort to ensure and maintain compliance with applicable data protection laws and principles.
This means that the personal data we hold about you must be:

- Used lawfully, fairly and transparently.
- Collected only for valid purposes that we have clearly explained to you and not used in any way incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- We will keep it as long as necessary for the purposes we have told you about.
- Kept securely.

## INFORMATION PROCESSING

Personal data (or personal information) means any information about a living individual from which that person can be identified.

It does not include data where the identity has been removed (anonymous data) or can no longer lead to identification (pseudonymised data).

It also does not include information about a legal person (for example, a company or other entity).

Special categories of more sensitive personal data require a higher level of protection.

### PERSONAL INFORMATION

We collect and maintain personal information about our staff, students, and visitors, including the personal information provided and obtained during the application and registration process.

We will generally collect, store, and use the following categories of personal data:

- Personal details such as your first name, surname, and title
- Personal contact details such as your home address (including postcode), mobile number, and personal email address
- Date of Birth
- Nationality (EU or Non-EU)
- Title
- Status of application (standard eligible application, mature or provisional)
- Bank account details
- Education History
- Academic transcripts
- Qualifications
- Unique student number (allocated by the Institute)
- IHRI email account

- IHRI student record, including your courses, modules, student assessments, assignments, work produced, examinations taken, examination results and grades, repeated units, progression reports, class ranking, degrees conferred and other information that may be included in your record
- Academic and extracurricular interests
- Feedback (including course resignation letters)
- Disciplinary information (reports and hearings)
- Information about your use of our information and communications systems.

Collection of Personal Information

We may collect personal data about you in several ways, including:

- From the information you provide when interacting with us before joining, for example, when you express an interest in studying at the Institute.
- When you apply to study at the Institute, complete our enrolment forms and other admissions processes and procedures.
- When you communicate with us by telephone, email or via our website, for example, to make enquiries or raise concerns and
- In various other ways as you interact with us as a student at the Institute.

How We Use Information About You

We will only use your data when the law allows us to.

Most commonly, we will use your data in the following circumstances:

1. Upon your consent (Article 6(1)(a), GDPR). The Institute will only process certain data if you give us express consent on specific occasions.1
2. Where it is necessary for the performance of your student agreement (Article 6(1)(b), GDPR).

The Institute will regularly need to process your data to meet its contractual commitments to you (the student), e.g., delivery of courses, teaching and assessment, and degree conferral.

## Situations in which we will use personal data

We need to process the categories of personal information above primarily for the following purposes.

(i) To perform your student agreement or due to legitimate interests

- Admission, registration, and administration of your studies
- Academic assessment and progression
- Administration of student-related policies and procedures, including appeals, complaints, grievances, disciplinary matters and conduct, cheating and plagiarism
- Academic matters, including the provision of our core teaching, learning and research services (for example, registration, assessment, attendance, managing progress, academic misconduct investigations, certification, and graduation)
- Billing
- Maintaining student records
- Providing library, IT, and information services
- Provision of student support services
- Organising teaching and examinations
- Collect tuition or other course (or module) fees (where applicable)
- Administer finance (e.g., fees and bursaries) (where applicable)

- Administration of student computing services
- Conferral and publication of awards and degrees
- Research and statistical analysis
- Creation and provision of a student email address
- Correspondence regarding lectures, tutorials, and seminars
- Direct mailing about
    - Institute activities and events organised for students,
    - Student benefits and opportunities offered by or through the Institute,
    - Career opportunities
- Provide career and other student support services
- Provide opportunities and placements with third-party organisations and businesses.
- Provide you with educational services which may not be set out in our student agreement but are nevertheless a part of our academic and educational mission.
- Monitor and evaluate the performance and effectiveness of the Institute, including by training our staff or monitoring their performance.
- Maintain and improve the academic, corporate, financial, estate and human resource management of the Institute.
- Enable effective communications with you
- To gather evidence for possible grievance or disciplinary hearings
- To deal with grievances and disciplinary action
- To manage internal disputes between you and other students or Institute employees
- To ensure network and information security, including preventing unauthorised access to our computer and communications systems and preventing malicious software distribution.
- To promote our services (e.g., providing information about student exchanges or other events happening);

(ii) To comply with a legal obligation

- To produce statistics and research for statutory reporting purposes
- To carry out audits (e.g., to ensure compliance with our regulatory and legal obligations)
- To assist with investigations (including criminal investigations) carried out by the police and other competent authorities; and
- We must comply with our other legal and regulatory obligations, as may be imposed on us occasionally, such as compliance with anti-money laundering laws and safeguarding requirements.

(iii) To establish, exercise or defend legal claims

- To deal with legal disputes which relate to or otherwise involve you, including accidents at our grounds and premises.
- For complaints and appeals procedures. Some of the above grounds for processing will overlap, and several grounds may justify our use of your personal information. These grounds may be updated from time to time.

These grounds may be updated from time to time.

<u>Failure To Provide Personal Information</u>

If you fail to provide certain personal information when requested, we may not be able to enforce your student agreement or comply with our legal obligations (such as safeguarding our students' welfare).

Change Of Purpose

We will only use your data for the purposes for which we have collected it unless we reasonably consider that we need to use it for another reason and where that reason is compatible with the original purpose. If we need to use your data for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so.

Data Sharing

Occasionally, we may need to share your data with certain third parties to achieve the processing purposes set out in this policy. We require all third parties to respect the security of your data and treat it according to the law. Indicative instances are as follows:

(i) To comply with a legal obligation

- Law enforcement authorities and regulatory bodies were, according to the investigation or disclosure of a potential crime.
- To national government departments and agencies where we have a statutory obligation to provide information (for example, the National Statistics Office, gathering of census information)
- To the National Statistics Office (NSO), government departments and other authorised users for the completion of student surveys and the analysis of student statistics and to enable them to carry out their statutory functions as applicable

(ii) To perform your student agreement or due to legitimate interests

- To external examiners for assessment
- To professional bodies where registration with that body is related to or a requirement of the student's studies
- To external bodies and individuals who have funded student prizes and awards
- To third parties who work with us to provide student support services (e.g. counselling)
- To banks (and other payment agencies you may use)
- To third parties who are contracted to provide out-of-hours IT services for us
- To organisations operating anti-plagiarism software on our behalf
- To professional and regulatory bodies (MFHEA) concerning the confirmation of qualifications, professional registration and conduct and the accreditation of courses
- To any organisation (data processor) acting under the Institute's authority to process personal data that it holds for the purposes set out.

(iii) To protect your vital interests

If you undertake a placement or complete a period of study with a third-party organisation or institution (e.g., an exchange visit), your personal data may be shared with the partner organisation or receiving institution to administer the placement and/or your studies at the receiving institution (as applicable).

Data Security

We have implemented measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your data according to our instructions and where they have contractually agreed to treat the information confidentially and keep it secure (duty of confidentiality).

We have implemented appropriate security measures to prevent your data from being accidentally lost, used, accessed in an unauthorised way, altered, or disclosed.

We have also established procedures to deal with any suspected data security breach.

We will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## Transferring Personal Data To A Country Outside The Eea

We may transfer any personal data we hold to a country outside the EEA for any of the purposes set out in this policy. Such transfers are restricted and must be based on a valid transfer mechanism under Chapter V of the GDPR. We will ensure that data subjects are afforded a level of protection essentially equivalent to that guaranteed by the GDPR.

Transfers may take place on the following legal bases:

- Adequacy Decision: Where the European Commission has determined that the destination country ensures an adequate level of data protection.
- Appropriate Safeguards: In the absence of an adequacy decision, transfers may be based on appropriate safeguards that provide enforceable rights and legal remedies for individuals. The primary safeguard we use is the 2021 Standard Contractual Clauses (SCCs) adopted by the European Commission.
- Transfer Impact Assessment (TIA): The use of SCCs is no longer sufficient on its own. For any transfer to a country without an adequacy decision, we are legally required to conduct a Transfer Impact Assessment (TIA) to evaluate the destination country's laws and practices concerning public authority access to personal data. The TIA will assess the effectiveness of the safeguards and, if necessary, identify and implement additional measures to ensure an essentially equivalent level of protection.
- Derogations for Specific Situations: For specific, non-repetitive transfers, we may rely on derogations under Article 49 of the GDPR, such as:
    - Explicit Consent: We will seek your explicit consent after we have informed you of the possible risks associated with the transfer due to the lack of adequate safeguards.
    - Contractual Necessity: The transfer is necessary for the performance of a contract between you and IHRI or to take pre-contractual steps at your request.
    - Public Interest: The transfer is necessary for important reasons of public interest.

## Data Retention

We will only retain your data for as long as necessary to fulfil the purposes for which we collected it. This means personal data will be destroyed or erased from our systems when it is no longer required. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your data, the purposes for which we process your data and whether we can achieve those purposes through other means, and the applicable legal requirements.

The retention of all personal data is governed by the IHRI Administration - Record Retention Policy (DOC084), which is in place to meet our legal obligations and justifiable business needs.

Once you are no longer a student at the Institute, we will retain and securely destroy your data following our data retention policy.

In some circumstances, we may anonymise your data so that it can no longer be associated with you, and we may use such data without further policy.

Rights Of Access, Correction, Erasure, And Restriction

You have the right to request information about whether or not we are processing your data and how and why it is being processed.

You may email dpo@ihri.edu.eu to request information and a copy of the personal data we process about you.

This right to access your data is without prejudice to the integrity and confidentiality of the personal data of other persons, and only your data may be divulged to you.

You have the right to request the correction or rectification of the personal data that we hold about you.

This enables you to have any incomplete or inaccurate data we hold about you corrected and/or updated. However, we need to verify the accuracy of your new data.

You have the right to request the erasure of your data.

This enables you to ask us to delete or remove personal information where there is no good reason for us to continue to process it.

You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

Most commonly, this will be where we require further processing of the personal data:

- to comply with a legal obligation to which we are subject
- to assert, exercise or defend legal claims (including possible future claims)

You have the right to object to processing your data where we rely on a legitimate interest (or those of a third party), and there is something about your situation which makes you want to object to processing on this ground.

You also have the right to object to our processing of your data for direct marketing purposes.

You have the right to request the restriction of data processing.

This enables you to ask us to suspend the processing of personal information about you, for example, if you want us to establish its accuracy or the reason for processing it.

You have the right to request that we transfer (data portability) your data to you or a third party you designate.

We will provide you or a third party you have chosen with your data in a structured, commonly used, machine-readable format.

Note that this right only applies to automated information you initially provided consent for us to use or where we used the information to perform a contract with you.

If you want to review, verify, correct, or request the erasure of your data, object to the processing of your data, or request that we transfer a copy of your data to another party, please contact our data protection officer in writing.

We may request specific information from you to help us confirm your identity and ensure your right to access the information in question (or to exercise any of your other rights).

This is another appropriate security measure that we apply to ensure that personal data is not disclosed to anyone who has the right to receive it.

Where you may have provided your consent to collect, process, and transfer your data for a specific purpose, you can withdraw your consent for that specific processing at any time.

To withdraw your consent, please contact our data protection officer at dpo@ihri.edu.eu.

Once we have received notification that you have withdrawn your consent, we will no longer process your information.

Your withdrawal will not affect the lawfulness of any processing we carried out before you withdrew your consent.

Following your graduation, our Alumni Office will use your data to keep you in touch with the Institute and our Alumni Network.

A snapshot of your data may also be used for training purposes. You can exercise your right to object.

## Changes to the Privacy Policy

The Institute reserves the right to modify this Privacy Policy at any time. The date when this policy was last updated is indicated at the start of this policy.

## Data Protection Officer

We have appointed a data protection officer (DPO) to oversee compliance with this policy. If you have any questions about this policy or how we handle your personal information, please contact the DPO at dpo@ihri.edu.eu.

You have the right to complain to the competent supervisory authority in your jurisdiction on data protection matters. In the case of Malta, this is the Information and Data Protection Commissioner ("IDPC") (https://idpc.org.mt/en/Pages/Home.aspx). We would appreciate the opportunity to deal with your concerns internally before you approach the supervisory authority, so please bring the matter to our attention at the first instance.

References

1. DOC008 Administration - Privacy Policy.docx
2. The CJEU judgment in the Schrems II case - European Parliament, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.p

df
3. International data transfers | European Data Protection Board, https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en
4. Art. 45 GDPR – Transfers on the basis of an adequacy decision - General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-45-gdpr/
5. New Standard Contractual Clauses - Questions and Answers overview - European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en
6. Data Protection Compliance - PwC, https://www.pwc.com/al/en/Data_Protection_Compliance.pdf
7. International Data Transfers: When and How to Perform a Transfer Impact Assessment, https://www.transatlantic-lawyer.com/international-data-transfers-when-and-how-to-perform-a-transfer-impact-assessment/
8. Top-10 do's and don'ts for service providers implementing the new SCCs with EU customers, https://iapp.org/news/a/top-10-dos-and-donts-for-service-providers-implementing-the-new-sccs-with-eu-customers
9. DOC084 Administration - Record Retention Policy.docx