Appendix 2: Privacy Notice for Students

General

We take your privacy very seriously. In order to help protect your privacy, a law has been passed that sets out rules for organisations to help keep information about you (such as your name, address and information about your life) safe. To help you understand what we are doing to protect this information, we have created this document (called a "Privacy Notice"). This Privacy Notice explains what information we collect about you, why we collect it and what we do with it.

In this Privacy Notice, we use some terms that appear in the law that you may not be familiar with. Some key ones to remember are:

Personal data: This means any information that can be used to identify a person that relates to them in some way. For example, information that identifies you (such as your name and when you were born), your contact details (such as your home address and email address), photographs, information about your educational progress, etc.
Process: Means anything, we might do with personal data, including using it, storing it, sending it to other organisations, and deleting it.
Controller: This is the person or organisation that is in charge of the way that it uses your personal data.
Data Protection Officer (DPO): This is the person HRUC who is in charge of making sure we comply with our duties under data protection law.
Information Commissioner's Office: Also known as the "ICO", this is the organisation that is responsible for regulating data protection in the UK. The ICO can fine organisations that do not follow the law on data protection and helps protect individuals. All organisations that use personal data have to answer the ICO.

If you have any questions about the way we use your personal data, please contact our Data Protection Officer:

The College's official contact details are: Data Protection Officer
HRUC - Uxbridge Campus Park Road
Uxbridge UB8 1NQ

Tel: +44 (0) 1895 853311
Email: dpo@hruc.ac.uk

From time to time, you will be asked to provide HRUC with personal information in order to become a student or a customer and use College systems and services. Unless required or permitted by law, we will always ask you before we use it for any other reason.
We process a variety of different types of your personal data . This includes:

- Your name and contact details, as well as other information to help us identify you, such as your date of birth.
- Educational records (this includes information about your attendance, your coursework and exam results).
- Information about any special educational needs you may have.
- Correspondence about you, such as emails or letters.
- Information about your safety and wellbeing.
- Photos (and videos) of you, including images of you taken from our CCTV cameras.

Some types of personal data are given extra protection in the law because it is particularly sensitive – these are called "special categories of personal data" and "personal data relating to criminal offences and convictions" (criminal offence data). The special categories of personal data are: race / ethnic origin; political opinions; religious beliefs; trade union membership; genetic information; biometric information (if it is used to identify you); health information; and information about someone's sex life or sexual orientation.

We only collect special categories of personal data and criminal offence data where the law allows

us to. We may collect:

Information about your religion or beliefs, for example if you have specific dietary requirements or need time for prayer.
Information about health, for example any allergies you may have, details of medication you need to take or a disability.
Biometric information processed automatically using our biometric recognition systems.

Where your personal data comes from

Some of the personal data we process comes directly from you, for example information you give to your teachers. We also receive your personal data from members of our staff (such as your teachers or our reception staff). Sometimes, we may receive your personal data from other organisations such as the local authority, the police, and the Department for Education (DfE).

The law says that we must collect certain information from you in order to provide you with an education. If we do not receive this information, we may not be able to provide you with a place at HRUC.

Data protection law says we must have a valid legal reason to process your personal data.

These are:

To comply with our legal obligations. For example, this applies when we are:
Following legal rules set by the DfE that require us to collect your personal data.
Complying with laws relating to attendance and monitoring/reporting on your progress.
Protecting you and providing you with appropriate care.
Measuring how well HRUC is doing in providing you with an education.

Because **we have a task to do that is in the public interest** (this means something we need to do in everyone's interest) or to allow us to carry out our official functions that we are required to carry out by law, for example:

- To safeguard you and our other students.
- To support your learning.
- To monitor the use of our IT systems to make sure they are being used appropriately and in accordance with HRUC policies' rules.
- Dealing with a complaint or carrying out an investigation.

Because we have a **"legitimate interest"** in using your personal data in a certain way, but only where we believe our need to use the data fairly outweighs any potential impact on your privacy. We only rely on this lawful basis when the way we need to process your personal data falls outside the scope of our official functions. For example, this may include:

- using your image for ID cards and for access to HRUC premises.
- using images, video and audio recordings for reasonable school purposes such as for HRUC publications.
- purposes such as obtaining insurance or asking for advice from someone outside HRUC (such as from our solicitors); and
- sharing information with third parties such as the police, when they are investigating a crime.

We need to process personal data as a matter of life and death (vital interests). For example, if there is a medical emergency.

We rely on your **consent**.

We do not usually rely on consent to process your personal data but occasionally we may want to

use it in a way that is completely optional for you. Examples of where we rely on consent include:

Where we would like to use biometric data (e.g. your fingerprints for cashless catering.)

If there are specific circumstances where your consent is required to use photographs or videos of you.

When we ask for your consent to use your personal data, remember:

- You are in control – you can say “no”.
- Even if you do consent you can always change your mind later.
- If you want to withdraw your consent, you can do this at any time, just contact our DPO using the above details.
- If you decide to withdraw your consent, that doesn’t mean that our use of your personal data before you stopped consenting is against the law.
- If we are relying on your consent to do something for you and you do not want to provide it (or withdraw it), we may not be able to provide you with what you have asked. We will let you know at the time if this is the case.

When we process special categories of personal data or criminal offence data, because it is so sensitive the law says we need to have an extra-legal reason to use it. These include:

Explicit consent: For example, we need this when we are using systems that use biometric data (such as fingerprints or facial recognition).

Vital interests: For example, to share information about your health with a doctor in a medical emergency.

Legal Claims or Judicial Acts: For example, if you are taking us to court, we may need to use your personal data to defend ourselves.

Reasons of Substantial Public Interest: For example, to share information with the police where this is necessary to protect you or another student.

Health or Social Care: For example, where it is necessary to share your personal data with health professional such as a therapist.

Public Health: For example, where information needs to be collected and used in connection with a public vaccination programme or in response to a pandemic such as the COVID-19 pandemic. Where this happens, the data is handled by a health professional or someone who by law must keep your information confidential.

Who we share your personal data with

We will only ever share your information outside HRUC where the law says we can or should. Examples of who we may need to share your personal data with include:

- Your family.
- The local authority.
- Organisations that help us run our colleges such as IT providers and organisations that handle payments.
- People whose job it is to help you, such as a nurse or counsellor.
- Examining bodies.
- Your next college if applicable.
- Our legal advisors, accountants and auditors (if we need to ask for advice).

If you are aged 13 and over, the law requires us to pass on certain information to the local authority

or youth support services that has responsibilities in relation to the education or training of 13-19-year-olds. Your parent or guardian can request that only your name, address and date of birth be passed by informing us.

We have a statutory obligation to pass information to the Education and Skills Funding Agency (ESFA). You can view a separate privacy notice from the ESFA on behalf of the Department of Education by following this link: https://www.gov.uk/government/publications/esfa-privacy-notice

Youth Support Services

We will also share certain information about students aged 16+ with the London Borough of Hillingdon or their commissioned youth support service provider as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, visit www.hillingdon.gov.uk.

Marketing

When you enquire or apply to join us, we will contact you to provide you with information about your application, our courses and the other benefits of joining the College. We will not share your details with any other organisation for marketing purposes. If you would not like to receive information about the College, please let us know, however, this may result in you not receiving important information to support your application.

Transferring your personal data to other countries

Occasionally we may need to transfer your personal data outside the UK. We may also use service providers based outside the UK or who may need to transfer your personal data outside the UK.

Whenever your personal data is transferred outside the UK, we take steps to make sure it continues to be protected as though it was in the UK. We do this by:

Wherever possible, only transferring to countries with an adequacy decision. This means that the UK Government has decided that these countries provide the same level or a higher level of protection to personal data as we do in the UK.

If the countries your personal data is being transferred to does not have an adequacy decision, we use one of the safeguarding measures available under data protection law, such as using contracts, i.e. Standard Contractual Clauses (SCCs).

If you would like more information about how we protect your personal data if it is transferred outside the UK please contact our DPO.

Automated Decision-Making and profiling

Automated decision-making is when a system uses personal data to make decisions about people without any human involvement. Profiling takes place when different aspects about a person (such as their behaviour, interests or personality) are analysed in order to make predictions or decisions about them. Automated decision-making does not have to involve profiling, though it often will.

We will not make decisions that will significantly affect you based solely on automated decision-

making (including profiling) unless the law allows it. If ever we do this, we will always let you know

How long will we process your data for?

Your information will be securely destroyed after it is no longer required, in accordance with our retention policy. We will keep some records for an extended period of time or permanently if we are legally required to do so. For example, we are required to retain information by the Education and Skills Funding Agency (ESFA) to prove funding and support audits. You can request a copy of this policy from the college's Data Protection Officer.

Security

We take security measures to protect your information including:

Limiting access to our buildings to those that we believe are entitled to be there (by use of passes, key card access and other related technologies)

Implementing access controls to our information technology, such as firewalls, ID verification and logical segmentation and/ or physical separation of our systems and information

Ensuring that paper-based data is kept securely.

Your rights and your personal data

You have the following rights with respect to your personal data:

The right to access information we hold on you through a Subject Access Request (SAR):

At any point you can contact us to request the information we hold about you, why we have that information, who has access to the information and where we obtained the information from.

Information must be provided for free in most (but not all) cases. There are no fees or charges for the first request but additional requests for the same data may be subject to an administrative fee.

Manifestly unfounded or excessive requests can be charged for or refused.

The deadline for the processing of information is 'within 1 month'. This deadline can be extended in certain cases.

Additional information must be supplied e.g. the College data retention periods and the right to have inaccurate data corrected.

If the College wishes to refuse an SAR, it will need to have policies and procedures in place and demonstrate why it has refused the request.

The right to correct and update the information we hold on you:

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

The right to have your information erased:

If you feel that we should no longer be using your data or that we are illegally using your data, you can request that we erase the data we hold.

When we receive your request we will confirm whether the data has been deleted or the reason why it cannot be deleted (for example because we need it for our legitimate interests or regulatory purpose(s)).

The right to object to processing your data:

You have the right to request that we stop processing your data. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have legitimate grounds to continue to process your data. Even after you exercise your right to object, we may continue to hold your data to comply with your other rights or to bring or defend legal claims.

The right to data portability:

You have the right to request that we transfer some of your data to another controller. We will

comply with your request, when it is feasible to do so, within one month of receiving your request.

The right to withdraw your consent to the processing at any time for any processing of data to which consent was sought:

You can withdraw your consent easily by telephone, email, or by post (see Contact Details above).

The right to lodge a complaint with the ICO.

These rights do not apply in all circumstances. Sometimes, others might be able to exercise these rights for you. This is only usually appropriate if you are unable to do this yourself and it is in your best interests, or with your consent. Remember, these are your rights.

How to complain

If you have a data protection concern that cannot or has not been resolved by the College, you have the right to raise it with the ICO. Complaints should be directed to the Information Commissioner by one of these methods:

Post: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Telephone: 0303 123 1113.

Web: https://ico.org.uk/make-a-complaint/

Changes to our Privacy Notice

We will update and change this Privacy Notice from time to time to keep it up to date and accurate. So, please check back to look for changes. If we make a big change then we will let you know, usually by email.