HRUC GDPR Appendix 3: Privacy Notice Staff General

HRUC is committed to protecting and respecting your privacy. This Notice sets out why and how we collect and use your personal data during and after your working relationship with us and who it might be shared with. It also explains the legal bases for our use of your personal data and your legal rights.

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

Who is this Privacy Notice for?

This notice is for prospective, current, and former staff engaged by HRUC. It is intended to apply to all academic and support staff, contractors, voluntary workers, interns, temporary workers, trainees, apprentices, visiting music teachers, any peripatetic workers and sports coaches. (It also applies to Governors).

What Information Does HRUC Collect?

The Data Controller of personal information about you is HRUC. This Privacy Notice has been prepared in accordance with the UK GDPR and Data Protection Act 2018.
HRUC collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the College
- information about your remuneration, including entitlement to benefits such as pensions and sick pay
- details of your bank account and national insurance number
- Biographical and social information such as marital status and dependents, interests and lifestyle, social circumstances, hobbies and interests, and any other personal data that you choose to provide.
- Next of kin contact details and emergency contact numbers.
- Information generated through your use of our information and communications systems, such as usernames and emails sent using your work accounts.
- information about your nationality and entitlement to work in the UK
- information about your criminal record as detailed within your Enhanced DBS
- details of your schedule (days of work and working hours) and attendance at work
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence

Certain categories of personal data are regarded by data protection law as more sensitive than others and is given additional protection. This includes 'special category personal data' and personal data relating to criminal offences or convictions. Special categories of personal data includes information

about your health, racial or ethnic origin, sexual life, sexual orientation, religious beliefs, political opinions, trade union membership, genetic information, and biometric data (where used for identification purposes).

Special categories of personal data

We routinely collect and use the following special categories of personal data:

- Information about your racial or ethnic origin, religious or philosophical beliefs, sexual orientation and health for equality and diversity monitoring.
- Trade union membership
- Information about health and medical conditions (for example, where we need to make reasonable adjustments to your work environment because of a medical condition or record sickness absence), including details of any absences (other than holidays) from work including time on statutory parental leave and sick leave;
- Biometric information for our biometric identification systems (used for cashless catering).

Criminal offence data

We may also collect and use information about criminal offences (such as information about criminal convictions or allegations) but only where the law permits, for example where we are required by law to carry out pre-employment checks and DBS checks.

The source of your personal data

We obtain your personal data from the following sources:

- Directly from you (for example, when you provide information to use as part of the recruitment process or during the course of your employment through our interactions and correspondence with you);
- From third parties such as an employment agency, referees (such as your former employer or educational establishment), our pension provider, HM Revenue & Customs, (social media, such as LinkedIn).

Consequence of failure to provide us with your personal data

Some of the information we collect from you is required by law or under contract. If you fail to provide us with certain information when requested, we may not be able to perform the contract we have entered into with you (or are attempting to enter into), such as paying you or providing you with a benefit, or we may be prevented from complying with our legal obligations such as ensuring the health and safety of our workforce.

This may, for example, result in the termination of an offer of employment or engagement.

Why Does HRUC Process Personal Data?

HRUC needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit and pension entitlements.

In some cases, HRUC needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to meet Keeping Children Safe in Education guidelines, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. It is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, HRUC has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the College to:

- run recruitment and promotion processes including checking your qualifications
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- operate and keep a record of Enhanced DBS checks to ensure Safeguarding requirements are met
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the College complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled
- ensure effective general HR and business administration
- provide references on request for current or former employees
- respond to and defend against legal claims
- Provide references for you if requested
- Help keep you safe and protect our property through CCTV monitoring of our premises
- maintain and promote equality in the workplace

Depending on the circumstances, we rely on the following lawful bases to process your personal data :

Necessary for performance of a contract: For example, we will need to process your contact details and financial information in order to comply with any contract of employment or contract for services we have with you.

Necessary for compliance with a legal obligation: For example, to provide information to HM Revenue & Customs, or if you are applying for a teaching position we are required by law to carry out due diligence checks with the Disclosure and Barring Service (DBS).

Public task: We need to process your personal data because HRUC has tasks to perform that are in the public interest or exercising official authority, both of which are laid down in law. For example:

- As a public authority HRUC will need to process your personal data in order to comply with its statutory function to provide education.
- HRUC needs information about its staff and other workers to run our colleges lawfully, safely and efficiently, safeguard our pupils, staff and visitors, keep our property, staff and pupils safe and comply with all of our legal, educational and regulatory duties and obligations.

Legitimate interests: we will process your personal data where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example:

- Where we need to use staff information for reasonable purposes such as obtaining insurance or seeking professional advice from a third-party professional.
- to use images, video and audio recordings of staff in and on our website or our social media channels for reasonable HRUC purposes.
- to monitor staff use of our IT systems to make sure they are being used appropriately and in

accordance with the law and our policies and procedures.
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

Recognised Legitimate Interests: we will process your personal data where it is necessary for certain legitimate interests deemed by the UK GDPR as "recognised", which means we do not have balance those interests with your interests and fundamental rights. For example, safeguarding our staff and pupils, assisting law enforcement agencies with their investigations, or sharing personal data with another public authority which is needed for the performance of that authority's public functions.

Consent: in most cases, we will not need your consent to use your personal data. However, there are a few occasions where we either need it or choose to ask for it, for example, where we use your personal data for the purpose of direct marketing.

Vital interests: rarely, we may need to process personal data of our staff and workers to protect you or someone else's life. For example, to share information about medical conditions that you may have with a doctor or hospital in the event of an accident.

We also need to process your **special category personal data** and/or criminal offence information (such as information about criminal convictions or allegations) for the following legal reasons:

- **Employment, social security and social protection:** where processing your personal data is necessary for performing obligations or exercising rights conferred on us or on you by law in connection with your employment, for example we process details of disabilities in order to make reasonable adjustments to enable you to work.
- **Explicit consent:** rarely, we will process special categories of your personal data if you have given us your explicit consent but only where consent is appropriate.
- **Vital interests:** rarely, we may need to process personal data of our staff and workers to protect someone's life. For example, to share information about medical conditions that you may have with a doctor or hospital in the event of an incident or accident.
- **Reasons of substantial public interest (with a basis in law):** we will process your personal data when it is necessary for reasons of substantial public interest with a basis in law, for example: to share information with the police or the local authority where this is necessary in order to safeguard a pupil's welfare; or for legal and regulatory purposes such as child protection; or investigating allegations of malpractice or unfitness to work with children; or diversity monitoring; or health and safety etc.
- **Legal claims:** we may need to process special categories of your personal data in connection with legal claims such as where a complaint or legal claim is brought against you or HRUC, or in order to investigate allegations.
- **Other reasons:** less commonly, we may need to process special categories of your personal data where you have **already made this information public** or for **health or social care purposes** (with a basis in law) or for **public health purposes** (with a basis in law), for example: where staff information needs to be collected and used in connection with a public vaccination programme; or in response to a pandemic such as COVID-19. Where this happens, the data is handled by a health professional such as a nurse or someone who the law says must keep your information confidential.

Who Has Access to Personal Data?

Your information will be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the area in which you work and IT staff if access to the data is necessary for performance of their roles.

HRUC shares your data with third parties to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The College may also share your data with third parties in the context of a sale of some or all its business. In those circumstances, the data will be subject to confidentiality arrangements.

HRUC also shares your data with third parties that process data on its behalf, in connection with

payroll, the provision of benefits and the provision of occupational health services. Your data is also included in Subject Access Request detail.

Information on the Current Video Surveillance Systems may be shared with a limited group as detailed in the CCTV Policy.

We may share your personal data with our insurers, accountants, legal advisors, and any individual appointed by HRUC to carry out an independent investigation.

We may share your personal data with public authorities and regulators that need to use your information for their own reasons. For example, we may be required by law to share some of your personal data with the local authority and the Department for Education, HM Revenue & Customs, the police, and the DBS Regulators that we may need to share your information with include the Teaching Regulation Agency, the Charity Commission and the Information Commissioner's Office. Where we share your information with these third parties in this way, the third party will become a data controller of your personal data.

We may share your personal data with others outside HRUC such as, former and prospective employers (for reference purposes).

Transferring your personal data to other countries

Occasionally we may need to transfer your personal data outside the UK, for example, where our service providers are located abroad. 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 measured available under data protection law, such as using contractual agreements.

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

How Does the College Protect Personal Data?

HRUC takes the security of your data seriously. There are internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. The College takes the following security measures to protect your information:

- 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.
- Where HRUC engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For How Long Does the College Keep Data?

HRUC will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out in the Retention Policy that can be found on the intranet.

Your data protection legal rights

Data protection law provides you with the following legal rights over your personal data:

- **The right of access:** You can ask us for a copy of the personal data we hold (this is often called a “subject access request”). This right always applies. There are some exceptions which means you may not always be entitled to a copy of all of your personal data that we hold.
- **The right to rectification:** You can ask us to correct any information we have about you if you think it is wrong or to complete information if you think it’s incomplete.
- **The right of erasure:** You can ask us to delete or destroy information about you in some circumstances, for example if our use of your personal data is illegal or if we no longer need it.
- **The right to restrict our use of your information:** You can ask us to limit what we are doing with your information in some circumstances, for example you can ask us to stop using your information if you think it is inaccurate while we are its accuracy.
- **The right to object:** You can object to what we are doing with your information in some circumstances. For example, if we are relying on “legitimate interests” to process your personal data or if you don’t want your personal data to be used for direct marketing purposes (e.g. sending you marketing emails).
- **The right to withdraw consent:** You always have the right to withdraw your consent to the processing of your personal data, if we are processing it on the basis of your consent.
- **The right to data portability:** You can ask us to transfer your information to another organisation in a format that makes it easy for them to use. This right only applies to personal data held on a computer, that we have received directly from you and where we are processing it on the basis of your consent or for a contract we have with you.

If you would like to exercise any of these rights, please contact Data Protection Officer, HRUC, Uxbridge Campus, Park Road, Uxbridge, UB8 1NQ. You can make a Subject Access Request by completing the organisation's form which is found within the HRUC Data Protection Policy.

What If You Do Not Provide Personal Data?

You have some obligations under your employment contract to provide HRUC with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide HRUC with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the College to enter a contract of employment with you. If you do not provide other information, this will hinder the College's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

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 Information Commissioner’s Office, the governing body for privacy and data protection. 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.

Email through their website **www.ico.org.uk**

Changes to this Privacy Notice

We will update and change this Notice from time to time to keep it up to date and accurate. We will always publish the most up to date version on the intranet. If we make a major change that affects your rights then we will let you know, usually by email.