

## Hull University Union

### PRIVACY NOTICE (GENERAL)

Hull University Union (HUU) respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data when you visit our websites and use our facilities. It tells you about your privacy rights and how the law protects you.

Please use the Glossary to understand the meaning of some of the terms used in this privacy notice.

#### 1. **IMPORTANT INFORMATION AND WHO WE ARE**

##### **Purpose of this privacy notice**

This privacy notice aims to give you information on how HUU collects and processes your personal data including through:-

- your use of our websites
- the purchase of goods or services, attendance at our events or otherwise doing business with us, and
- visiting our premises and/or the use of our facilities, including details of our CCTV usage.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This is a general privacy notice for users of our website and facilities. We also have separate privacy notices for individuals such as employees, job applicants and students. This privacy notice supplements our other notices and is not intended to override them.

##### **Controller**

Hull University Union Limited is the data controller and responsible for your personal data.

We have appointed a manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact us using the details set out below.

Name of data privacy manager: Kevin Pearson

Email address: kevin.pearson@hull.ac.uk

Postal address: Hull University Union (HUU), Student Central, Cottingham Road, Hull, HU6 7RX

Telephone number: 01482 466265

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. If you have concerns we would, however, appreciate the chance to deal with the matter before you approach the ICO so please contact us in the first instance.

## Your duty to inform us of changes

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

## Third-party links

Our websites may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

## 2. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender and images of individuals recorded by CCTV cameras.
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.
- **Financial Data** includes bank account and payment card details. However, for online purchases we record your Identity and Contact Data but do not record payment card details. This information is collected through CardSave Community (Subsidiary of WorldPay UK Limited), our online payment card provider. No card payment details are stored through our website.
- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us or events attended.
- **Technical Data** may include internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our websites.
- **Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage Data** includes information about how you use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We may also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature in order to improve the content of our services.

We do not collect any **Special Categories of Personal Data** via our websites (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

### **If you fail to provide personal data**

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with our services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

### **Children**

We do not structure our websites to attract children. Accordingly we do not set out to collect personal data from anyone under 18 years of age unless they are students of the University of Hull.

It is however possible that children may be recorded on CCTV within our public areas if attending our site.

### **3. HOW IS YOUR PERSONAL DATA COLLECTED?**

We use different methods to collect data including through:

- **Direct interactions.** You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email, via our websites or otherwise. This includes personal data you provide when you:
  - purchase our products or services;
  - subscribe to our services or publications;
  - request marketing or other information to be sent to you;
  - do business with us;
  - enter a competition, promotion or survey; or
  - give us some feedback.
- **Automated technologies or interactions.** As you interact with our website and apps, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, and other similar technologies. Please see our cookie policy for further details: <https://www.hullstudent.com/about-us/cookie-policy>
- **CCTV images recorded on or around our premises.** Please see the section on CCTV below.
- **Third parties or publicly available sources.** We may receive personal data about you from various third parties such as (for students of the University of Hull) from the University under a data sharing agreement; Technical Data from analytics providers; Contact, Financial and Transaction Data from providers of technical, payment and delivery

services; and Identity and Contact Data from publicly available sources such as Companies House and the Electoral Register in the UK.

#### 4. **HOW WE USE YOUR PERSONAL DATA**

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- 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.
- Where we need to comply with a legal or regulatory obligation.

Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to direct marketing at any time.

#### **Purposes for which we will use your personal data**

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data.

<b>Purpose/Activity</b>	<b>Type of data</b>	<b>Lawful basis for processing including basis of legitimate interest</b>
To register you as a new customer	(a) Identity (b) Contact	Performance of a contract with you
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)

<p>To enable you to partake in a prize draw, competition or complete a survey</p>	<p>(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications</p>	<p>(a) Performance of a contract with you  (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)</p>
<p>To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)</p>	<p>(a) Identity (b) Contact (c) Technical</p>	<p>(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise)  (b) Necessary to comply with a legal obligation</p>
<p>To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you</p>	<p>(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical</p>	<p>Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)</p>
<p>To use data analytics to improve our website, products/services, marketing, customer relationships and experiences</p>	<p>(a) Technical (b) Usage</p>	<p>Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)</p>
<p>To make suggestions and recommendations to you about goods, services or events that may be of interest to you</p>	<p>(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile</p>	<p>Necessary for our legitimate interests (to develop our products/services and grow our business)</p>

Please see the separate section below relating to our CCTV usage.

## **Marketing**

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising. We have established the following personal data control mechanisms:

### Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services, events and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us or purchased goods or services from us or if you provided us with your details when you entered a competition or registered for a promotion and, in each case, you have not opted out of receiving that marketing.

### Third-party marketing

We will get your express opt-in consent before we share your personal data with any third party for marketing purposes.

### Opting out

You can ask us or third parties to stop sending you direct marketing messages at any time by contacting us at any time.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase, product/service experience or other transactions.

### Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **5. CCTV**

We currently use CCTV cameras to view and record individuals on and around our premises. The images of individuals recorded by CCTV cameras are personal data and therefore subject to the data protection legislation.

We currently use CCTV around our site as outlined below. We believe that such use is necessary for legitimate business purposes, including:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- for the personal safety of staff, students, visitors and other members of the public and to act as a deterrent against crime; and
- to support law enforcement bodies in the prevention, detection and prosecution of crime

This list is not exhaustive and other purposes may be or become relevant.

## **Monitoring**

CCTV monitors all public areas of the building both internal and external. In addition to CCTV, security staff and Duty Managers wear body worn cameras during club and live events which captures both image and sound.

One fixed CCTV camera also records sound and this unit is located in the secure room in Asylum nightclub which is used as an interview room following incidents in the club.

Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring.

## **Operation of CCTV**

Where CCTV cameras are placed, signs are displayed to alert individuals that their image may be recorded.

We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. This may include HR staff involved with disciplinary or grievance matters and security personnel. Recorded images will only be viewed in designated, secure offices.

## **Retention and erasure of data gathered by CCTV**

Data recorded by our CCTV system will be stored but will not be retained indefinitely and will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough for the purposes of any investigation and subsequent legal proceedings. In cases where there is no need to keep the data for a longer period, images will be kept for no longer than 31 days. At the end of their useful life, all images will be erased permanently and securely.

## **Covert Monitoring**

We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

In the unlikely event that covert monitoring is considered to be justified, the decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

## **6. DISCLOSURES OF YOUR PERSONAL DATA**

We may have to share your personal data with External Third Parties as set out in the Glossary for the purposes set out in the table at section 4 above.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal

data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

Data from CCTV cameras will not normally be released to a third party unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced. In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime. We will maintain a record of all disclosures of CCTV footage.

## **7. INTERNATIONAL TRANSFERS**

We do not currently propose to transfer your personal data outside the European Economic Area (EEA).

In the event that in future we need to transfer your personal data out of the EEA, we will ensure that relevant legal safeguards are in place or are implemented.

This policy shall be updated in the event that we intend to transfer personal data out of the EEA.

## **8. DATA SECURITY**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

## **9. DATA RETENTION**

How long will you use my personal data for?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

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 personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax and/or legal purposes.

Our policy on retention of data from CCTV cameras is set out in section 5 above.

Details of other retention periods for different aspects of your personal data can be requested by contacting us.

In some circumstances you can ask us to delete your data: see below for further information.

## **10. YOUR LEGAL RIGHTS**

Under certain circumstances, you have rights under data protection laws in relation to your personal data, as follows:-



**Request access** to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

**Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

**Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

**Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

**Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

**Request the transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

**Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

*If you wish to exercise any of the rights set out above, please contact us.*

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

#### What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

## Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

## **GLOSSARY**

**CCTV:** means fixed and domed cameras designed to capture and record images of individuals and property.

## LAWFUL BASIS

**Legitimate Interest** means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

**Performance of Contract** means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

**Comply with a legal or regulatory obligation** means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

## THIRD PARTIES

### **External Third Parties**

- Third Parties specifically referred to in the section headed “Disclosure of your Personal Data.”
- Service providers acting as processors who provide card payment services, support services, shipping and IT, software and system administration services.
- Professional advisers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities based in the United Kingdom who require reporting of processing activities in certain circumstances.
- The University of Hull for matters relating to students studying at the University.