HUSU – Data Protection Policy

Document Owner:	HUSU	**Date Created:**	September 2021
Document Author:	Finance & HR Director	**Version:**	1
Approved By:	Senior Leadership Team	**Date:**	September 2021

Revision History

Version	Revision Date	Section Revised	Reason for Revision	Description of Revision
1	September 2021	All	GDPR Review	Full review of all documentation

INTRODUCTION

a) This Policy sets out how Hull University Students' Union handles the Personal Data of our members, customers, suppliers, employees, workers and other third parties.

b) This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present members, employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

c) This Policy applies to all employees, workers, contractors and directors. You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the Hull University Students' Union to comply with applicable law. Your compliance with this Policy is mandatory. Any breach of this Policy may result in disciplinary action.

d) This Policy (together with any related policies and guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Hull University Students' Union Data Processing Manager (DPM).

SCOPE

a) The DPM is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines. That post is held by the Finance & HR Director (Tel: 01482 466265).

b) Please contact the DPM with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPM in the following circumstances (which is not an exhaustive list):

i. if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Hull University Students' Union) (see *Section 4* below);

ii. if you are unsure about the retention period for any Personal Data (see *Section 8* below);

iii. if you are unsure about what security or other measures you need to implement to protect Personal Data (see *Section 9* below);

iv. if there has been a Personal Data Breach (*Sections 9 and 10* below);

v. if you need any assistance dealing with any rights invoked by a Data Subject (see section 12);

vi. whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a Data Protection Impact Assessment (DPIA) (see *Section 16* below) or plan to use Personal Data for purposes other than what it was collected for;

vii. if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see *Section 17* below);

viii. if you need help complying with applicable law when carrying out direct marketing activities (see *Section 18* below); or

ix. if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (see Section 19 below).

PERSONAL DATA PROTECTION PRINCIPLES

a) We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

i. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

ii. Collected only for specified, explicit and legitimate purposes (Purpose Limitation);

iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

iv. Accurate and where necessary kept up to date (Accuracy);

v. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

vi. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality). vii) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation);

vii. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests);

b) We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

LAWFULNESS, FAIRNESS, TRANSPARENCY

a) **LAWFULNESS AND FAIRNESS**

i. Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

ii. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

iii. The GDPR allows Processing for specific purposes, some of which are set out below:

(1) the Data Subject has given their Consent;
(2) the Processing is necessary for the performance of a contract with the Data Subject;
(3) to meet our legal compliance obligations;
(4) to protect the Data Subject's vital interests;
(5) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

iv. We must identify and document the legal ground being relied on for each Processing activity.

b) **CONSENT**

i. A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

ii. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

iii. Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

iv. Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

v. You will need to evidence Consent captured and keep records of all Consents so that Hull University Students' Union can demonstrate compliance with Consent requirements.

c) **TRANSPARENCY (NOTIFYING DATA SUBJECTS)**

i. The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

ii. Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPM, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice or Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data.

iii. When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

iv. You must use the Company's standard Privacy Notices/Fair Processing Notices if you are required to issue these documents in the course of carrying out your role. If you are unsure as to which document to use you should contact the DPM.

5) PURPOSE LIMITATION

a) Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

b) You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

6) DATA MINIMISATION

a) Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

b) You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

c) You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

d) You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Hull University Students' Union data retention guidelines.

7) ACCURACY

a) Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

b) Where your role involves Processing you should ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards and take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8) STORAGE LIMITATION

a) Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

b) You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

c) The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Hull University Students' Union's guidelines on data retention.

d) Where your role involves Processing you should:-

i. take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable; and

ii. ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

9) SECURITY INTEGRITY AND CONFIDENTIALITY

a) **PROTECTING PERSONAL DATA**

i. Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

ii. We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks. This may include, but is not limited to, data security measures such as password protection, encryption, restrictions on storage of data on certain devices and restrictions on who can access certain areas of our computer systems or physical areas of our premises.

iii. All employees, workers, contractors and directors are responsible for protecting the Personal Data we hold and must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

iv. You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

v. You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(1) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
(2) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
(3) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

vi. You must comply with and not attempt to circumvent the safeguards we implement in order to protect Personal Data.

10) REPORTING A PERSONAL DATA BREACH

a) The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

b) We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

c) If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. **Immediately** contact the person or team designated as the key point of contact for Personal Data Breaches, namely the Finance & HR Director. You should preserve all evidence relating to the potential Personal Data Breach.

11) TRANSFER LIMITATION

a) The GDPR restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

b) Due to the special conditions which apply to the transfer of personal data outside the EEA you must refer to the DPM before carrying out any such transfer.

12) DATA SUBJECT'S RIGHTS AND REQUESTS

a) Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

i. withdraw Consent to Processing at any time;
ii. receive certain information about the Data Controller's Processing activities;
iii. request access to their Personal Data that we hold;
iv. prevent our use of their Personal Data for direct marketing purposes;
v. ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
vi. restrict Processing in specific circumstances;
vii. challenge Processing which has been justified on the basis of our legitimate interests or in the public interest; request a copy of an agreement under which Personal Data is transferred outside of the UK;
viii. object to decisions based solely on Automated Processing, including profiling (ADM);
ix. prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
x. be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
xi. make a complaint to the Information Commissioner's Office; and
xii. in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

b) You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

c) You must immediately forward any Data Subject request you receive to the Finance & HR Director.

13) ACCOUNTABILITY

a) As a Data Controller the Hull University Students' Union must have adequate resources and controls in place to ensure and to document GDPR compliance.

14) RECORD KEEPING

a) The GDPR requires us to keep full and accurate records of all our data Processing activities.

b) Where your role involves Processing you should maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Company's guidelines.

15) TRAINING AND AUDIT

a) You must undergo all mandatory data privacy related training as required by Hull University Students' Union and (for managers and supervisors) ensure your team undergo similar mandatory training.

b) You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

16) DATA PROTECTION IMPACT ASSESSMENT (DPIA)

a) Data controllers must conduct DPIAs in respect to high risk Processing.

b) You should conduct a DPIA (and discuss your findings with the DPM) if you are tasked with implementing major system or business change programs involving the Processing of Personal Data including use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes).

c) A DPIA must include:

   i. a description of the Processing, its purposes and the Company's legitimate interests if appropriate;

   ii. an assessment of the necessity and proportionality of the Processing in relation to its purpose;

   iii. an assessment of the risk to individuals; and

   iv. the risk mitigation measures in place and demonstration of compliance.

d) If you are required to conduct a DPIA and require assistance or guidance, please refer to the DPM.

17) AUTOMATED PROCESSING AND AUTOMATED DECISION-MAKING (ADM)

a) Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

   i. a Data Subject has Explicitly Consented;

   ii. the Processing is authorised by law; or

   iii. the Processing is necessary for the performance of or entering into a contract.

b) If certain types of Sensitive Data are being processed, then grounds (ii) or (iii) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

c) A DPIA must be carried out and the consent of the DPM received before any Automated Processing (including profiling) or ADM activities are undertaken.

18) DIRECT MARKETING

a) We are subject to certain rules and privacy laws when marketing to our customers.

b) For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

c) The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

d) A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

e) You must comply with any Hull University Students' Union guidelines in place in relation to direct marketing to customers.

19) SHARING PERSONAL DATA

a) Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

b) You may only share the Personal Data we hold with another employee, agent or representative of any of our group companies if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

c) You may only share the Personal Data we hold with third parties such as our service providers if:

i. they have a need to know the information for the purposes of providing the contracted services;

ii. sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

iii. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

iv. the transfer complies with any applicable cross border transfer restrictions; and a fully executed written contract that contains GDPR approved third party clauses has been obtained.

20) CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time without notice to you so please check regularly to obtain the latest copy of this Policy.

ACKNOWLEDGEMENT OF RECEIPT AND REVIEW

I acknowledge that I have received and read a copy of Hull University Students' Union Data Protection Policy and understand that I am responsible for knowing and abiding by its terms.

This Policy does not set terms or conditions of employment or form part of an employment contract.

Signed .....

Printed Name .....

Date .....

GLOSSARY

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer or Data Protection Manager (DPO/DPM): A DPO is the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, a DPM has been nominated. This is the person assigned with the responsibility for data protection compliance.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action). **United Kingdom General Data Protection Regulation (UK GDPR):** the General Data Protection Regulation (*(EU)*

2016/679). Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, onetime privacy statements covering Processing related to a specific purpose.

Processing or Process: 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 transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.