# GDPR Record of statement

***For the:*** *University of Portsmouth Students' Union*
***Last updated:*** *8th November 2023*
***Approved by:*** *Finance and Risk Committee (November 23)*

## Introduction

The University of Portsmouth Students' Union ("The Union" or we") is a charitable organisation whose registered address is The Student Centre, Cambridge Road, Portsmouth, Hampshire, PO1 2EF. This address are securely locked and alarmed when not occupied.

Our primary purpose is the advancement of education of students at the University of Portsmouth through the delivery of our charitable objects.

We have approximately 37 employed staff and over 2,000 volunteers based from the above premises. The Union stores and processes some of its data remotely:

- University of Portsmouth managed servers (K Drive) - minimal storage via this method now.
- Google who provide G-Suite Services
- Meteoric Web Servers for self-hosted platforms
- Cloud-based platform providers Xero, Shopify, Kayako, Deputy, Qualtrics and Ticket Tailor
- Committee member and volunteer personal laptops

All of the above are data processors to the Union as data controller. We have GDPR compliant processor contracts or agreements in place with all of the above named parties (except committee members and volunteers who undertake our GDPR training).

The Union has sought legal and professional advice on matters of GDPR from commercial law specialists at Warner Goodman LLP and the Information Commissioner's Office. This document and the processes established in managing our data compliance has had oversight and guidance from their specialists and the Students' Union Finance and Risk Committee.

## Policy Statement

1. The Union intends to comply with GDPR as defined in the Data Protection Act 2018- The UK's implementation of the General Data Protection Regulation (GDPR)

2. We will therefore:

    a. Only process as much personal data as is necessary for our administration and the services we supply.

    b. Only hold such data for so long as necessary for those purposes. In this connection we have decided that ten years following the last contact with an individual is usually an appropriate period to hold data covering the legal limitation period (six years) and a moderate margin. As in most cases this is only archived data, not sensitive, not dangerous and will not be used there seems little risk to data subjects.

    c. Only process such data on grounds for lawful processing provided within GDPR Article 6 (Section 8 of the Data Protection Act 2018)

    d. Send or otherwise provide appropriate notices (GDPR Articles 13 and 14) to those whose personally identifiable information ("Personal Data") is processed by us including our employees, volunteers and individuals or individuals within partners who supply us with goods or services. We will also send such notices to individuals within organisations to whom generic marketing communications (eg newsletters) are sent.

    e. Not engage in direct marketing to clients or prospects otherwise than in accordance with the relevant legislation and guidance from the ICO.

    f. Utilise appropriate organisational and technical measures to ensure that Personal Data processed by us is kept secure.

    g. Where we use third party data processors we will choose them carefully with a view to their data security and compliance with GDPR and have GDPR compliant contracts with them.

    h. Not transfer Personal Data (which includes giving third parties access to it within our IT system) to recipients located outside the European Economic Area and the UK without confirmation from our Data Protection Officer that such transfer is lawful.

    i. Update this document from time to time so that it remains an accurate record of our data processing activities and policies.

3. The Head of Marketing and Engagement is appointed as our Data Protection Officer.

4. GDPR is not intended to require us to treat employees of our current or prospective partners and suppliers whose contact details we are required to use for dealing with those organisations, nor individuals who contact us intending to engage in correspondence with us, as data subjects to whom we should send notices pursuant to Articles 13 and 14, merely because we hold and use those contact details in connection with our dealings with them or their employers, or keep copies of such communications, as the effect of such interpretation would be disproportionate.

5. Where we hold and process such personal data for the purposes of direct marketing to those individuals' employers we should, unless guidance from the ICO says otherwise, either:

    a. obtain consent to that direct marketing from the individuals and send the notices required by Articles 13 and 14 to the individuals; or

    b. be satisfied that we have a legitimate interest in holding that Personal Data and using it for that purpose.

6. When employee, trustee or members data is shared with our pension provider, insurance provider, HMRC, BUCS and National Governing Bodies they are neither our processor nor joint controller of the data concerned as it is being provided for their own use as they see fit to provide a service to us and/or benefits to our employees and members. We will however, where possible, require contracts with them containing confidentiality obligations in respect of that data and other data that they create relating to our employees, members or customers in the context of the work they are doing.

7. In partnership with the University of Portsmouth, who collect our membership data as part of their enrollment process and responsibilities for enabling the Education Act, we have determined that we are a joint controller of this data. Through being a joint controller we are able to share membership data as appropriate between both organisations. We have a data sharing agreement in place, reviewed and signed off annually with the University of Portsmouth.

8. The Information Commissioner's Office has advised us that in joining a specific club or society which is linked to special categories of personal data (such as LGBT+, Labour Students or ISOC) it would only be an assumption that the person was providing information about their sexuality, political or religious beliefs and as such would not come under the special category of personal data.

## Our processing

1. **Full and affiliate members (Associate removed in Bye Law Changes 2023)**

| | |
|---|---|
| **Personal data collected:** | Student ID, Email Address, Full Name, Faculty, Department, Course, Year of Study, Level of Study, Mature Student, PT or FT Status, DL Status, Domicile, Graduation Year, Fee Paying Status, Parent/Carer, Telephone, Images of the Individual, Postal Address, Group Membership, Date of Birth, Age, NI Number, DVLA Number, Signature, Next of Kin Details and Course Instance Location |
| **Special categories of data collected:** | Ethnicity and Gender |
| **Data origination:** | University of Portsmouth, Student Directly |
| **Storage location:** | K Drive, Qualtrics,, CCTV Control Units), G-Suite, Xero, Shopify and iZettle |
| **Identified data usage:** | Membership records, advice centre user records, CCTV meeting minutes, records of attendance at events, event attendance, purchase history, elections & referenda voting history, democratic engagement history, registered driver details, newsletter subscriptions, inbound and outbound payments, refunds, retail purchase history, group membership, course rep records, research engagement, have your say idea engagement, health and safety records, medical records and society registration history |
| **Third parties with access:** | University of Portsmouth, National Governing Bodies, BUCS, Portsmouth Mediation Service and Endsleigh |
| **Retention period:** | 10 Years |

## 2. Customers and visitors

| | |
|---|---|
| **Personal data collected:** | Image of individual, Postal Address, Telephone, Email Address, Full Name and Student ID |
| **Special categories of data collected:** | None |
| **Data origination:** | Provided by individual |
| **Storage location:** | K Drive, Qualtrics,, CCTV Control Units), G-Suite, Xero, Shopify and iZettle |
| **Identified data usage:** | CCTV, Event ticket sales history, inbound and outbound payments, refunds and retail purchase history |
| **Third parties with access:** | None |
| **Retention period:** | 10 Years |

## 3. Employees of suppliers, contractors and clients

| | |
|---|---|
| **Personal data collected:** | Email Address, Full Name, Business Name, Postal Address, Role Title, Telephone, Signature and Bank Details |
| **Special categories** | None |

| | |
|---|---|
| **of data collected:** | |
| **Data origination:** | Provided by individual |
| **Storage location:** | Xero, Locked Filing Cabinet and G-Suite |
| **Identified data usage:** | Client invoices, supplier payments, marketing and communications, credit management and fraud prevention |
| **Third parties with access:** | Blue Spire (Auditors), Counter Culture (Financial Advisors). |
| **Retention period:** | 10 Years |

## 4. Employees of the Union

| | |
|---|---|
| **Personal data collected:** | Email Address, Full Name, Telephone, Postal Address, Role Title, Date of Birth, NI Number, Bank Details, P45 / P46, Next of Kin Details, Disciplinary Record, Financial Bonding, Photographic ID, Business Interests, Family Relationships, Right to work in UK, Reference Personal Details, Course, Year of Study and Student ID |
| **Data origination:** | Provided by individual |
| **Special categories of data collected:** | Gender, Criminal Record and Personal Health Records- Upon application on staff applications we ask for the following and then remove after 6 months for right of appeal: Race, gender, sexual orientation and disability. |
| **Storage location:** | Locked Cabinet, Barclays Bank, Deputy, G-Suite, K Drive and Xero |
| **Identified data usage:** | Employee Administration, Recruitment processes and Expense claims |
| **Third parties with access:** | Blue Spire, Counter Culture, Warner Goodman, National Health Service |
| **Retention period:** | Recruitment records - 6 weeks after not being appointed to a role<br>HR records - Indefinitely |

## 5. Data Storage

The Union stores and processes some of its data remotely:

- University of Portsmouth managed servers (K Drive)
- Google who provide G-Suite Services
- Meteoric Web Servers for self-hosted platforms
- Cloud-based platform providers Xero, Vend, Kayako, Deputy, Qualtrics and Ticket Tailor

All of the above are data processors to the Union as data controller. We have GDPR compliant processor contracts/agreements in place with all of the above named parties. All processors undertake to keep the data within the EEA or are compliant and certified under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

## 6. Organisational and technical measures

We use the following organisational and technical measures to ensure the confidentiality of personal data:

a. Provisions that employees and volunteers who process data are required to consider the use of lockable filing cabinets, secure storage for archived files and the use of a shredder or confidential waste bin for hard copies of paperwork, file notes, incoming and outgoing letter correspondence containing personal data.

b. For electronically held data employees and volunteers who process data are required to consider using storage on the University network, work g-suite or platforms approved by the Data Protection Officer, password protection on all files containing personal data, the use of the Union's secure platforms for processing data, running up to date antivirus and malware systems, installation of adequate firewalls, the secure destruction or disposal of IT equipment.

c. CCTV units are not networked and access to the systems are through password protected platforms. This data may only be accessed by those authorised by the Data Protection purposes or law enforcement agencies.

d. Email accounts are individually assigned and not shared with colleagues or third parties. Access to emails are only authorised for third parties for specific purposes by Senior Management Team members.

e. The data protection and information security handbook provides clear guidance on data sharing, data handling, security breach procedures and disposal of data.

f. We hold GDPR compliant contracts with all data processors.

g. All employees and volunteers undertake training in data privacy law and cyber security before being given authorised access to process data held by the Union.

## 7. Consent

We do not engage in direct marketing to individuals except in their capacity as a member of our organisation or as a conduit for our trading company.

Following consultation with the ICO and a review of the appropriate legislation we have concluded that as our members have purchased through their tuition fees a membership of the Union we do not need consent in communicating through digital means with our members about our related charitable products and services. We believe that as a member there is a legitimate interest in receiving this information which is noted as a lawful reason for processing data in Recital 47. In all communications there is an opt-out and the member

will have received an article 13 or 14 notice prior to receiving any communications at all.

Where the Union is undertaking campaigning, lobbying, communicating a political standpoint or acting as a conduit for commercial marketing activities (undertaken by our subsidiary trading company on behalf of third party clients) explicit consent shall be obtained.

The Union follows industry guidance relating to research gathering. Where personal data is collected as part of a research exercise this shall be undertaken with the explicit consent of the individual.

We are aware that consent under GDPR must be freely given, specific, informed and unambiguous given by a statement or a clear affirmative action and that we have to keep a record of each consent obtained for as long as we are using it. We do not currently believe that any of our processing of Personal Data, except for the sending of the commercial marketing and research activities, requires data subject consent.

**8. Legitimate Interests**

Recital 47 of the GDPR reads: *"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."*

We rely on legitimate interest as justifying much of our processing of Personal Data as we have assessed that the majority of our processing activity would be in the reasonable expectations of those we process data about. Our activities reliant on legitimate interest are as follows:

a. **Employees:** We require the data processing to enable us to be a good employer and pay employees. Whilst they are candidates we require it to assess them for employment. Employees and candidates expect us to hold and process that personal data for those purposes. We destroy candidate personal data if the candidate is unsuccessful.

b. **Members:** As a membership organisation processing individual data is central to our service provision. Members are able to opt-out of processing by terminating their membership. To provide a high standard of service and personalise our provision we record and process data relating to members engagement and communications preferences. The maximum study term for a student is 7 years and we retain student data for a further 3 years to a maximum of 10 years. Our data is refreshed annually by the University.

c. **Suppliers, partners and clients:** Our suppliers, partners and customers are not usually individuals so here we are dealing with the identifiable employees of our suppliers and clients who require us to deal with such individuals or self employed individuals. We require their personal data (email, office address, telephone numbers) to enable us to contact them in the context of their job. If an employee leaves a client or supplier we remove their details from the CRM and other systems (or we would be communicating with the wrong person). They expect that we will hold their contact details for this purpose.

d. **Customers:** When individuals purchase products or utilise services through our trading company we have access to process this data to administer our contracted duties and send them carefully selected information about our products and services.

In all the above cases we believe that we have a legitimate interest in carrying out that processing and that the processing has no significant risk to the rights and freedoms of the individuals concerned.

**9. The Education Act**

Together with the University of Portsmouth we have interpreted the act requires all University of Portsmouth students to be members unless they opt-out which revokes any requirements to receive explicit consent for data processing in relation to the administration of membership.

**10. Members**

We are satisfied that our activities serve a legitimate interest to our members and do not risk the rights and freedoms of the individuals concerned. We are required to deliver certain services by the Education Act for our members. Our members are informed of our processing activities an Article 14 notice served at enrollment.

We hold next of kin/emergency contact details in respect of our members. This is authorised under Article 6.1 (d) GDPR as the processing is necessary to protect the vital interests of the member.

**11. Employees**

We are satisfied that we only process employee Personal Data where we have a legitimate interest in so doing and are changing/have changed our contracts of employment and staff handbook to make this clear and include the necessary notices.

We hold next of kin/emergency contact details in respect of employees. This is authorised under Article 6.1 (d) GDPR as the processing is necessary to protect the vital interests of the employee.

Following advice from Warner Goodman, we have determined that other than Blue Spire (for Payroll purposes) all Third Parties with access to employee data are simply recipients and not required in any way to process this data on behalf of the Students' Union.

**12. Notices**

As noted elsewhere we do not believe that GDPR should be interpreted as requiring an Article 13 or Article 14 notice to be sent to every data subject whose personal data we are processing. We do believe that such notices should be sent to:

- Suppliers and clients once engaged with the Students' Union
- Our employees
- Identifiable employees, members, University staff or attendees of minuted meetings

**13. Processors**

We have identified the following parties as data processors:

- Portsmouth Mediation Service - In the provision of mediation services for students
- University of Portsmouth - In the provision of managed servers (K Drive)
- Google - In the provision of G-Suite applications
- Meteoric - In the provision of Students' Union website servers
- Facebook Workplace - In the provision of an intranet service
- Xero - In the provision of accounting software
- Kayako - In the provision of case management and customer relationship management
- Deputy - In the provision of staff rota management
- Qualtrics - In the provision of research tools
- Ticket Tailor - In the provision of ticketing services
- Shopify- In the provision of payments

The above parties either have a direct contract using the Students' Union model contract or through GDPR compliant terms and conditions of use of service.

The Students' Union shares data with National Governing Bodies for legitimate purposes.

**14. Joint Controllers**

We conclude that we are joint controllers with the University of Portsmouth in data shared to manage our members, course representatives and those identified within meeting minutes. We are taking measures with the University of Portsmouth to document the arrangements required by GDPR.

**15. Third Party Partnerships**

We have identified that the Students' Union works with several key partners to undertake the delivery of services and activities on behalf of the charity. It is our opinion that Third Parties

do not act as data processors of Students' Union data unless identified in section 13. Partners are required to have appropriate data protection policies where they process data on the Students' Union behalf with the exception of Portsmouth Students' Union Trading Company Ltd which is considered a financial conduit for Students' Union commercial work and simply a recipient of data not a processor or controller.
gia
We have taken the view that all guidance, policies and procedures applicable to the Students' Union are also applicable to Portsmouth Students' Union Trading Company Ltd. These policies may be read as those of the trading company as well as the charity.

Retail, Event and Advertising services are delivered on behalf of the Students' Union by Portsmouth Students' Union Trading Company Ltd as a commercial conduit. When considering marketing these services it is understood that they form part of the charity's service provision and therefore the soft opt-in exemption applies as a legitimate interest. We consider this statement applicable to all third parties where the services appear to be delivered by the Students' Union despite being licensed to a third party for delivery.