John Moores Students' Union

Data Protection Policy

Approved by the Trustee Board	**19/11/2024**
Date of Next Review	**19/11/2027**
Author	**Sarah Latham (Deputy CEO – Membership Engagement)** **Paul Chapman (CEO)**

Contents

1. General Statement of Policy

John Moores Students' Union (JMSU) is committed to ensuring the privacy and security of personal data in compliance with data protection laws, including the UK GDPR and the Data Protection Act 2018. JMSU values the trust placed in it by its members, employees, volunteers, clients, suppliers, and partners, and is dedicated to processing personal information lawfully, fairly, and transparently. The Union implements robust measures to safeguard data from unauthorized access, loss, or damage, and this policy applies to all individuals and entities who handle data on behalf of JMSU. All are expected to understand and follow their responsibilities to protect personal data in line with this policy.

2. Scope

This policy aims to clearly outlines JMSU committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well as safeguarding the rights and freedoms of persons whose information the organisation may process pursuant to the UK General Data Protection Regulation 2020 (UK GDPR), the Data Protection Act 2018 (DPA) and any other applicable legislation.

This policy applies to all employees, volunteers, student staff and officers of the organisation including contractors, subcontractors and consultants, and any other partners that have access to data held by, or on behalf of JMSU.

3. Aims & Objectives

The aims and objectives of this policy are as follows:

- **Legal Compliance** - To ensure that JMSU processes all personal information in compliance with data protection laws, including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This includes the lawful collection, processing, storage, and disposal of personal data.
- **Transparency and Trust** - To maintain transparency with all stakeholders about how their personal information is used, stored, and shared. The policy aims to foster trust between JMSU and those whose personal data is handled by clearly communicating data handling practices.
- **Data Security** - To safeguard all personal data from unauthorised access, accidental loss, destruction, or damage by implementing appropriate technical and organizational measures. The policy also ensures that data breaches are identified, reported, and resolved in a timely manner.
- **Data Minimisation & Accuracy** - To ensure that only the necessary and relevant personal data is collected, processed, and retained, and that such data is kept accurate and up to date.
- **Data Rights and Support** - To provide guidance and support to employees, volunteers, and officers in handling personal data. It also aims to inform individuals of their rights concerning their personal information, including their rights to access, rectification, erasure, and data portability, as well as how to lodge complaints if needed.

4. Governance

4.1 Data Protection within JMSU is the responsibility of the Trustee Board. The Board oversees the development, implementation, and monitoring of the policy. The Board ensures that the Union maintains high standards of data protection, accountability, and transparency.

4.2 On a day-to-day basis, the Trustees have delegated responsibility for the implementation of this policy to the Chief Executive Officer.

4.3 The job titles referred to in this Policy are subject to change. If there is any doubt about designated roles, the CEO can give final clarification.

5. Definitions

5.1 Liverpool John Moores University Students' Union, here after referred to as 'the organisation,' 'the Union' or with the abbreviation 'JMSU.'

5.2 **Legislation:** UK General Data Protection Regulation 2020 (UK GDPR), the Data Protection Act 2018 (DPA) and any other applicable legislation. In this document, all such legislation is collectively referred to as 'data protection legislation'.

5.3 **Personal data:** means any information that identifies, directly or indirectly, a data subject.

5.4 **Data subject:** refers to any living person who is the subject of personal data held by the organisation. A data subject must be identifiable by name, ID, address, online identifiers, or other factors such as physical, physiological, genetic, mental, economic, or social factors.

5.5 **Data controller:** the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

5.6 **Data processor:** a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

5.7 **Data Protection Officer (DPO):** DPOs assist an organisation to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding relevant policies, procedures and practice and act as a contact point for data subjects and the Information Commissioner's Office (ICO).

5.8 **Data Protection Lead/accountable person:** is a member of the organisation's staff who oversees data protection obligations and procedures.

5.9 **Information Commissioner's Office (ICO):** The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

5.10 **Processing:** refers to any action taken in relation to personal data including, but not limited to, collection, adaptation, alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination, or deletion, whether by automated means or otherwise.

5.11 **Special categories of data:** racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, biometric data (where used for identification purposes), data concerning health, data concerning a person's sex life or sexual orientation.

6. Duties & Responsibilities

6.1 DATA PROTECTION OFFICER

6.1.1 The Data Protection Officer (DPO), if appointed, holds specific delegated authority for overseeing compliance with data protection laws and this policy. The DPO ensures that JMSU is informed of its obligations, monitors internal processes, provides guidance, and acts as the main point of contact for data subjects and the Information Commissioner's Office (ICO). If no DPO is appointed, these responsibilities fall to a designated member of the SLT.

6.1.2 The organisation has appointed Hope & May as the Data Protection Officer which will be overseen internally by Chief Executive Officer. They can provide advice and guidance on data protection matters and should be your point of contact for any data breaches or subject access requests (see sections 10 and 11).

6.1.3 The Data Protection Officer is responsible for the implementation and updating of this Data Protection Policy.

6.2 **JMSU STAFF**

6.2.1 Staff must ensure all personal data is processed lawfully, fairly, and transparently in line with legislation and JMSU's policies.

6.2.2 Staff are responsible for safeguarding personal data from unauthorised access or breaches and must report any potential data security issues immediately.

6.2.3 Staff must ensure data subjects' rights, including access, rectification, and erasure, are respected, and promptly addressed.

6.3 **DEPARTMENTAL MANAGERS**

6.3.1 Managers are responsible for ensuring that appropriate procedures, systems, and resources are in place to implement the policy and uphold data protection standards across the Union.

6.4 **THIRD PARTY (Contractors, Subcontractors, Consultants, and any other partners)**

6.4.1 Third parties must adhere to all data protection clauses written in any contract or agreement with JMSU. This includes but is not limited to, keeping confidential any data they access as part of their work with the Union. They will comply with this policy, or we will ensure their data protection policy aligns with this policy.

7. Seven Principles of Data Protection

7.1 JMSU is committed to adhere to Article 5 of the UK GDPR which lists the seven principles of data protection:

7.1.1 **Lawfulness, fairness, and transparency:** the organisation is committed to process data lawfully, fairly and in a transparent manner.

7.1.2 **Purpose limitation:** the organisation collects personal data for specified, explicit and legitimate purposes. The organisation doesn't further process data in a manner that is incompatible with those purposes.

7.1.3 **Data minimisation:** the organisation is committed to process data that is adequate, relevant, and limited to what is necessary.

7.1.4 **Accuracy:** personal data is kept accurate and up to date.

7.1.5 **Storage limitation:** the organisation is committed to keeping personal data for no longer than necessary.

7.1.6 **Integrity and confidentiality:** the organisation processes data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

7.1.7 **Accountability:** the organisation is able to demonstrate compliance.

7.2 JMSU complies with the principles in the following ways:

7.3 **LAWFUL, FAIRNESS, & TRANSPARENCY**

7.3.1 **Lawful Basis -** JMSU identifies a lawful basis every time they process personal data. (See section 8 for more information on the six lawful bases for processing data).

7.3.2 **Privacy Notice -** JMSU is committed to informing all data subjects about the processing of their data beforehand so that they are able to make an informed decision about whether or not to provide that data. A full privacy notice is made available to anyone who wants to know more about how the organisation processes data. JMSU has complied with Articles 13 and 14 of the UK GDPR which lists the content that needs to be included in the privacy notice. JMSU may periodically change how personal data is processed. JMSU will inform the data subjects, accordingly, as required by the data protection legislation. Please see ***Appendix C.***

7.4 **PURPOSE LIMITATION**

7.4.1 JMSU collects personal data for specified, explicit and legitimate purposes, and the data is not further processed in a manner that is incompatible with those purposes.

7.4.2 The organisation may extend a purpose to cover new processing, as long as the new purpose is compatible with the old. Compatibility is measured according to 'reasonable expectation' the data subject may have. The organisation needs to process information to carry out its work, meet objectives and comply with its contractual obligations. The organisation will only ever collect information that is needed in order to carry out its work, improve its services, report to contract holders and partners, fulfil any requests that data subjects make, personalise services to best meet data subjects' needs, and keep track of the impact and quality of the organisation's work.

7.4.3 The purpose of the data processing is included in the privacy notice and in the Record of Processing Activity (ROPA) spreadsheet which is maintained and reviewed regularly.

7.5 **DATA MINIMISATION & ACCURACY**

7.5.1 The Union is committed to the quality of the data that it collects and processes. This means that the data must be:

a. Adequate
b. Relevant
c. Limited to what's necessary.
d. Accurate
e. Kept up to date.

7.5.2 The ROPA spreadsheet keeps a log of the personal data processed for each category of data subject, and where that data is stored. It also identifies staff members who are responsible for updating or deleting data from the different sources of storage.

7.5.3 The organisation is aware of the importance of collecting and maintaining accurate personal data. JMSU receives student data from LJMU via a daily transfer, thus ensuring it receives the most up-to-date information. The organisation will assume that any information submitted by data subjects is accurate at the date of submission. Data subjects are promptly informed via the privacy notice that they are responsible for ensuring that the personal data held by the organisation is accurate and up to date.

7.5.4 All staff members are required to update the organisation as soon as reasonably possible of any changes to their own personal information to ensure records are always up to date.

7.5.5 JMSU shall, on an annual basis, carry out a review of all personal data controlled by the organisation and decide whether any data is no longer required to be held for the stated purposes, and where required arrange for that data to be deleted or destroyed in accordance with the requirements of the Data Protection Legislation.

7.6 STORAGE LIMITATION

7.6.1 JMSU will not keep data longer than is necessary. When the organisation no longer needs it, it will dispose of information securely.

7.6.2 Personal data is retained according to a retention schedule and then destroyed or deleted in a secure manner as soon as the retention date has passed. In some cases, retention periods will be based on legal consideration. In other cases, the reason may be more practical or based on organisational decisions. The retention schedule is logged in the ROPA spreadsheet and data subjects are informed via the privacy notice how long their data will be kept.

7.6.3 Data that is kept for long periods of time is examined and amended, if necessary.

7.6.4 Should any personal data be required to be retained beyond the retention period set out in the ROPA, this may only be done with the express written approval of the Data Protection Officer and must be in line with data protection requirements.

7.7 INTEGRITY & CONFIDENTIALITY

7.7.1 JMSU maintains appropriate, technical, and organisational security to protect personal data from unauthorised access or intrusion.

7.7.2 The organisation limits access to the data only to those employees, contractors and partners who need such access according to their role and job requirements.

7.7.3 The organisation will strive to train its employees, trainees, volunteers, and freelancers about its data protection practices.

7.7.4 IT Terms & Conditions and Security Measures

7.7.4.1 There are several IT measures that JMSU puts in place to help ensure the security of its data, including (but not limited to):

a. Providing staff with email guidance and training, ensuring they are aware of when to use the BCC function (e.g. when sending emails to more than one student)
b. Using strong passwords
c. Using multi-factor authentication where possible
d. Regularly updating software
e. Using secure wi-fi and avoiding the use of unsecured public wi-fi

7.7.4.2 For more information on security measures and IT provisions, please refer to LJMU's IT terms and conditions.

7.7.5 Physical Security Measures

7.7.6.1 There are also several physical security measures that JMSU puts in place, including (but not limited to):

a. Clear desk policy to avoid people leaving confidential data on their desk.
b. Locked filing cabinets, drawers, or lockers for confidential paperwork.
c. Automatic screen shut down when staff members are away from their desk.
d. Arrangements for shredding paper.
e. Shredding and disposing of manual records which have passed their retention as 'confidential waste.'
f. Printing of records containing personal data should be avoided whenever possible.

7.7.6 **Confidentiality**

7.7.6.2 All employees of the organisation are responsible for keeping secure any personal data controlled by the organisation. Under no circumstances may any personal data be disclosed to any third party unless the organisation has provided express authorisation, or has entered into a confidentiality agreement, a data processor agreement, or a data sharing agreement with the third party (see section 12 for information about these agreements). Data must not be used, copied, or distributed for any purpose other than as required for the performance of their duties within the scope of their employment with JMSU.

7.7.6.3 Upon termination of the Employee's employment, or upon request by JMSU, the Employee agrees to promptly return all documents, materials, and other tangible embodiments of confidential information, or to destroy such materials if requested by the Employer, and to certify such destruction in writing.

7.7.6.4 Employees acknowledge that any breach of this policy may result in irreparable harm to JMSU and may be subject to legal action, including claims for damages and/or injunctive relief. Any negligible or deliberate breach may result in disciplinary action being taken, in serious cases being considered gross misconduct.

7.8 **ACCOUNTABILITY – DEMONSTRATING COMPLIANCE**

7.8.1 In accordance with lawful requirements, the organisation keeps records so that they can demonstrate the steps taken to comply with the UK GDPR:

a. **Record of Processing Activities (ROPA)** spreadsheet identifies information such as the category of personal data processed for each data subject, the lawful basis of the processing, data retention, data storage, who is responsible for the data, and who has access to the data.

b. **The Activities, Incidents, and Risks** reporting spreadsheet keeps a log of key information such as discussions and decisions about data protection, identified risks, any personal data breaches and response, training of staff and volunteers, requests to exercise any rights by data subjects and management of those requests, notifications to the ICO.

c. **Legitimate Interests Assessments (LIAs)** that have been carried out (see section 8 for more information).

d. **Data Protection Impact Assessments (DPIAs)** that have been carried out to justify the approach where processing poses particular risks (such as processing of special category of data) – see section 13 for more information.

e. This **Data Protection Policy** which includes most procedures relating to data protection.

f. **Privacy Notice** for data subjects.

g. **Data Processing Agreements** with external providers and other data processors (see section 12 for more information).

h. **Data Sharing Agreements** (also called information sharing protocol) with other data controllers or joint controllers (see section 12 for more information)

i. **Appropriate Policy Document** which may be completed in some circumstances outlined by the Data Protection Act (2018) when processing special categories of data or criminal records.

7.8.2 Department/area heads alongside the Data Protection Officer will be responsible for ensuring the maintaining of records. Department/area heads must report to and update the Data Protection Officer on the processing of personal data within their department/area.

8. The Six Lawful Bases for Processing Data

8.1 JMSU processes personal data by identifying a 'lawful basis' chosen from the six possibilities set out in Article 6 of the UK GDPR:

a. with the **consent** of the data subject
b. for a **contract** involving the data subject
c. to meet a **legal obligation**
d. to protect any personal **vital interests**
e. for **government** and **judicial functions**
f. in the organisation's **legitimate interests** provided the data subject's interests are respected

8.2 The most common lawful bases that the organisation identifies are consent, contract, legal obligation, and legitimate interest. The lawful bases for the different processing activities are recorded in the Record of Processing Activities (ROPA) spreadsheet which is maintained and reviewed regularly.

8.3 **CONSENT**

8.3.1 If JMSU chooses consent as its lawful basis, it means that the data subject has given their consent to the processing of their personal data for one or more specific purposes. The organisation will gather proof of that consent to demonstrate that the data subject has consented to processing of their personal data (as per Article 7.1 of the UK GDPR). The data subject has the right to withdraw their consent at any time (as per Article 7.3 of the GDPR).

8.3.2 Consent to the processing of personal data by the data subject must be:

a. Explicit i.e. demonstrated by active communication between JMSU and the data subject and must not be inferred or implied by omission or a lack of response.
b. Freely given and should never be given under duress when the data subject is in an unfit state of mind or provided on the basis of misleading or false information.

c. Specific and informed, it should cover the controller's name, the purposes of the processing and the types of processing activities.
d. A clear and unambiguous indication of the wishes of the data subject

8.3.3 In relation to sensitive data, consent may be provided in writing. If given verbally, this must be acknowledged in writing.

8.3.4 The organisation understands that Consent is for the time being and may review and refresh consent as appropriate.

8.3.5 Consent will not be the condition for processing data where a service or product is purchased.

8.4 **CONTRACT**

8.4.1 JMSU identifies contract as its lawful basis when processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering a contract.

8.5 **LEGAL OBLIGATION**

8.5.1 JMSU identifies legal obligation as a lawful basis when processing is necessary for compliance with a legal obligation to which the controller is subject.

8.6 **LEGITIMATE INTEREST**

8.6.1 If JMSU chooses legitimate interest as its lawful basis, a Legitimate Interest Assessment may be completed in order to show what the Union's interest is and that it is legitimate, to show why the processing is necessary in pursuing this interest, to consider the potential impact on any data subjects' rights and freedoms and to measure whether the data subject might reasonably expect JMSU to process their data. An opt-out option may be made available to the data subject. Data subjects always have a right to object to the processing of their data.

8.7 **ADDITIONAL MEASURES**

8.7.1 When data processing poses particular risks, such as the processing of special category data the organisation will complete a Data Protection Impact Assessment (DPIA) to justify their data protection approach.

8.7.2 When processing special category data or criminal records without the consent of the data subject, data protection law requires controllers to identify another lawful basis under Article 6 of the UK GDPR other than consent, supported by one of the exemptions of Article 9 (2) which might need to be further supported by the Data Protection Act (2018). When processing criminal records, the lawful basis identified in Article 6 needs to be additionally supported by the Data Protection Act (2018). The organisation may complete an Appropriate Policy document for the processing of special category data and criminal data without consent of the data subjects as required by law.

9. Data Subjects and the Data JMSU Collects

9.1 JMSU collects personal information from different groups of data subjects:

a. Members & Associate Members (as per Membership byelaw)
b. Volunteers
c. Job Applicants
d. Employees
e. Trustees
f. Volunteer External Partners
g. Freelancers/External Consultants
h. Web & Social Media Data Subjects
i. Guests

9.2 The Union's privacy notice and ROPA will explain the different kinds of data it collects and the lawful basis for processing them. JMSU processes normal category data and may also collect special category data and criminal data.

9.3 For more information on how JMSU processes special categories of data and criminal records, please see section 8.

10. Data Breach

10.1 Article 4.12 of the UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, authorisation, and authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.' A breach could damage JMSU's reputation and its relationship with stakeholders or expose the University, its staff, or students to risks including fraud, identity theft and distress.

10.2 If a breach occurs, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

10.3 Please see ***Appendix A*** for a step-by-step guide to the procedures that staff must follow when they are made aware of a data breach.

10.4 Where JMSU share data with other organisations, the agreements or contracts that are in place include a clause requiring them to inform JMSU within 24 hours of them becoming aware of a breach. This is to allow JMSU to make a report to the ICO within 72 hours if required. Other parties may also be subject to appropriate legal action in accordance with these agreements made. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred immediately to the relevant authorities.

10.5 If a data subject has been harmed by a breach, they can take the controller to court for compensation.

10.6 Any data breaches by staff will be carefully investigated and dealt with through the Union's disciplinary policy and could be considered as gross misconduct given the level of importance. Please see JMSU's Disciplinary Policy for further information.

11. Data Subject Rights

11.1 JMSU is fully aware of the data subject rights described in Articles 15 - 22 of the UK GDPR, and these are listed in the privacy notice. The data subjects' rights include:

a. The right to be informed.
b. The right of access
c. The right of rectification

d. The right to be forgotten (erasure)
e. The right to restrict processing.
f. The right to data portability
g. The right to object processing
h. Rights in relation to automated decision making and profiling.

11.2 Additional rights of data subjects include:

a. The right not to receive direct marketing.
b. The right to claim damages should they suffer any loss as a result of a breach.
c. The right to complain and the right to request that the ICO conduct an assessment.

11.3 If data subjects wish to exercise any rights, they can contact the organisation at jmsudpo@ljmu.ac.uk. They are reminded of their rights and how to exercise them in the privacy notice they receive.

11.4 All staff members are trained to recognise an incoming request to exercise any right, to understand when the right applies and to pass it on without delay to the designated person.

11.5 All requests from data subjects to exercise any rights are recorded into the 'Activity, Incident and Risk reporting spreadsheet.'

11.6 Under certain circumstances, mostly described in Schedules 2-4 of the Data Protection Act (2018), the Union may not need to comply with the request by a data subject to exercise one of their rights.

11.7 Those circumstances will be assessed on a case-by-case basis and outlined in ***Appendix B.***

12. Data Sharing – Working with Other Organisations

12.1 As with any other organisation, JMSU may collaborate with:

a. data processors
b. joint controllers
c. separate controllers

12.2 All third parties we work with who have or may have access to personal data of our data subjects will either comply with this policy, or we will ensure that their data protection policy aligns with this policy.

12.3 **DATA PROCESSORS**

12.3.1 A data processor is a company, organisation or individual who is not an employee or volunteer, that processes data on behalf of the data controller (JMSU in this policy).

12.3.2 Before deciding to use a particular service, the Union would check the terms and conditions and decide whether it is compliant before deciding to use that service.

12.3.3 With freelancers, external researchers and IT companies for example, the Union stipulates a Processing Agreement, or a contract including data protection provisions, as outlined by Article 28.3 of the UK GDPR.

12.3.4 JMSU remains responsible for what happens to the data and remains liable for any mistakes of the data processors. In the contract with the data processor, the Union may include a provision that requires the data processor to reimburse JMSU.

12.4 **JOINT CONTROLLERS**

12.4.1 Article 26 of the UK GDPR defines joint controllers as 'two or more data controllers which jointly determine the purpose and means of processing'. When JMSU collaborates with a data controller, the parties must agree to a Joint Controller Agreement which could include the following:

a. who it applies to
b. general data protection principles, including the basic principle of confidentiality.
c. the purposes for which information will be shared.
d. the lawful basis on which sharing will take place.
e. how each partner will discharge their transparency obligations, and whether all parties will use the same form of words to ensure consistency
f. procedures for sharing information, and in particular for obtaining and recording consent from the data subject (if this is the lawful basis).
g. procedures to ensure that all parties have the same understanding of how to comply with the data protection principles regarding data quality and retention.
h. access and security procedures.
i. procedures for ensuring that the handling of data subjects' rights is consistent and fully compliant.
j. procedures for raising concerns or resolving difficulties.
k. how the agreement will be managed and kept under review

12.4.2 The purpose for which information will be shared, the lawful basis on which the sharing will take place and general information about each data controller will need to be included in the privacy notice for those data subjects affected by the data sharing and collaboration between the organisation and the joint controller.

12.5 **SEPARATE CONTROLLERS**

12.1.1 The organisation may collaborate with another organisation which is a separate controller, as information is merely disclosed to one other. In this case, the Union may agree to a Data Sharing Agreement with the other separate controller(s), which defines the following:

a. parties involved in the agreement.
b. purpose for which information will be shared.
c. the lawful basis on which the sharing will take place.
d. other organisations involved in the data sharing.
e. what data items will be shared (including special category data)
f. procedures to comply with data subjects' rights.
g. governance arrangements

12.1.2 The purpose for which information will be shared, the lawful basis on which the sharing will take place and general information about each data controller will need to be included in the Privacy notice for those data subjects affected by the data sharing and the collaboration between the organisation and the other separate controller(s).

13. Compliance Obligations

13.1 **RISK ASSESSMENT**

13.1.1 Risk Assessment is an important part of the accountability of an organisation. It is vital that the Union is aware of all risks associated with personal data.

13.1.2 It is the policy of the organisation not to transfer or share data into an environment that is not considered compliant with UK or EU data protection law.

13.1.3 Where personal data processing is carried out using new technologies, or when a high risk is identified in relation to the rights and freedoms of natural persons, the organisation is required to engage in a risk assessment of the potential impact, also known as a 'Data Protection Impact Assessment' (DPIA). More than one risk may be addressed in a single DPIA. The organisation has developed and agreed upon a procedure for completing a DPIA. This procedure is always followed where there is a need to measure risk. The procedure is completed by the Data Protection Officer.

13.1.4 In addition to this, and if the outcome of a DPIA points to a higher risk than the organisation intended and personal data processing could result in distress and/or may cause 'damage' to the data subjects, it is for the Data Protection Officer to decide whether the organisation ought to proceed, and the matter should be escalated. In turn, the Data Protection Officer may escalate the matter to the regulatory authority (prior agreement) if significant concerns have been identified.

13.2 **DATA PROTECTION BY DESIGN & DEFAULT**

13.2.1 This policy includes procedures in relation to data protection across the organisation, involving different staff members, teams, and delivery. As the organisation aims towards full compliance, and therefore also towards a data protection "by design and by default," these procedures will be embedded into the operating guidance as appropriate.

13.2.2 The goal of this principle would mean that in the organisation, everyone who starts a new project or sets up a system or process must ensure that they incorporate data protection as a matter of course, consulting the Data Protection Officer. Consideration of the data protection implications should be a standard check point before any project or system is signed off.

13.3 **INTERNATIONAL DATA TRANSFER**

13.3.1 If personal data is stored outside of the UK and the EU, safeguards to protect personal data may include, but are not limited to, the UK Addendum used in conjunction with the EU Standard Contractual Clauses (SCCs), or UK International Data Transfer Agreement (IDTAs). Such safeguards will be subject to Transfer Risk Assessments (TRAs).

13.4 **REGISTRATION TO THE ICO**

13.4.1 The organisation has registered with the Information Commissioner as it engages in the processing of personal information identifying data subjects directly or indirectly.

13.4.2 ICO Registration Number: ZB694682

13.4.3 The organisation pays an annual fee to the ICO, as required by law.

13.5 **COOKIES POLICY**

13.5.1 Please view our cookie policy in ***Appendix 3*** to understand the different cookies we use on our website.

14. Inspection & Audit Review

14.1 This Policy is updated regularly by the Data Protection Officer when required. It is reviewed annually by the Data Protection Officer and the board of trustees.

14.2 An annual report on data protection will be produced by JMSU for consideration by the Board of Trustees. This report will include information to help the Trustee Board compare JMSU's decision-making over time.

15. Related Policy

15.1 This policy should be read in conjunction with the following policies and documents:

a. Confidentiality agreement
b. Safeguarding policy
c. Privacy notice
d. IT terms and conditions

15.2 JMSU Policies can be found at https://www.jmsu.co.uk/what-we-do-how-we-work/our-policies

16. Appendix A – Data Breach Procedure

If a breach occurs, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence. Please see below for a step-by-step guide to the procedures that staff must follow when they are made aware of a data breach:

- Any staff member who discovers or suspects a personal data breach is required to immediately inform their line manager and the Data Protection Officer, and with support from their line manager, complete the breach reporting form which is saved teams (GDPR Hub). It's important to report it as soon as possible.

- The staff member and/or their line manager need to ensure that the breach is not still occurring and take any immediate mitigating action that may reduce the impact of the breach.

- In conjunction with Article 33.1 of the UK GDPR, the organisation must report the data breach to the ICO within 72 hours 'unless the personal data breach is unlikely to result in a risk to the rights and freedom of natural persons'. The decision to report such a breach will be made by JMSU. If the breach is reported, the Data Protection Officer will make the report using the ICO's website.

  Factors that may determine whether a breach is reportable include:

  i. sensitivity of the categories of data, e.g. data identifying a health condition.
  j. quantity of data concerned.
  k. whether there is a potential for a high risk of harm to the data subjects concerned

  Mitigating factors that may be considered when not reporting a breach include:

  a. the data is retrievable.
  b. there is evidence that data has been contained and that those who may have access will not process the data in such a way as to cause harm or distress to the data subjects concerned.

- If the data breach is reported to the ICO, the organisation will make available any documents or records that the ICO requires to peruse the inquires. The organisation will cooperate with the ICO with any request and record any guidance the ICO gives in accordance with the breach in the 'activity, incident and risk reporting spreadsheet' (please see section 7 for more information on this spreadsheet).

- If the data breach is likely to result in a high risk to the rights and freedoms of natural persons (e.g. where the breach could result in ID theft or fraud; physical harm; significant humiliation and/or damage to reputation) the organisation would need to communicate the breach without undue delay to the affected individuals. In some circumstances, the organisation may decide to not inform the individuals if by doing so it would cause more damage and anxiety to the data subjects than the data breach itself.

- If the individuals are informed of the data breach, the organisation will also ask if they want to log a formal complaint to the ICO regarding how their personal data has been managed.

- The Data Protection Officer logs the data breach into the 'activity incident and risk reporting spreadsheet' in order to identify lessons the organisation can learn and the changes that can be made. If the data breach is reported to the ICO, the case number supplied by the ICO will be recorded in the spreadsheet.

- Train staff where required to ensure the breach doesn't happen again**.**

17. Appendix B – Exceptions to Data Subject Rights Requests

Under certain circumstances, mostly described in Schedules 2-4 of the Data Protection Act (2018), the Union may not need to comply with the request by a data subject to exercise one of their rights. Those circumstances will be assessed on a case-by-case basis.

1. **The right to be informed**

   Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The organisation is committed to comply with this right and they do so via the privacy notice.

2. **The right of access and SAR procedure**

   A data subject has the right to make access requests in respect of personal data that is held and disclosed. To understand how we deal with Subject Access Requests, please view our SAR policy.

3. **The right of rectification**

   JMSU is aware of the provisions in Article 16 of the UK GDPR - if the data subject becomes aware that the organisation is holding incorrect information about them, they have the right for it to be corrected, and if their information is incomplete, they can also submit additional information to be added.

4. **The right to be forgotten (erasure)**

   If a data subject asks the organisation to delete their information, as stated in Article 17 the organisation will do so without undue delay when:

   a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed.

b. the data subject withdraws consent (if that is the basis on which the processing is taking place), and where there is no other legal ground for the processing.
c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing.
d. the personal data has been unlawfully processed.
e. the personal data has to be erased for compliance with a legal obligation.
f. the personal data has been collected in relation to the offer of online services to a child.

In addition, if the organisation has made the information public, the organisation must try to have it erased in other locations as well. In conjunction with Article 19 of the UK GDPR, the organisation informs anyone to whom data has been disclosed, unless this 'proves impossible or involves disproportionate effort'. The organisation will also inform the data subject which recipients their data has been disclosed to, if they ask

There are exceptions to the 'right to be forgotten' for reasons relating to freedom of expression, public health, archiving, research and statistics, legal claims, and legal obligation.

There may also be circumstances where the organisation has no choice but to retain data, for example to mark a record for suppression to ensure that no direct marketing is sent to that individual in the future.

The organisation will process a request for erasure without undue delay, and within one month of receipt.

5. The right to restrict processing

The data subject shall have the right to restriction of processing of their personal data where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
- the processing is unlawful, and the data subject opposes the erasure of the personal data, requesting the restriction of its use instead.
- the controller no longer needs the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise, or defence of legal claims.
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

6. The right to data portability

This right applies when processing is based on consent, or a contract between the organisation and the data subject, and the processing is taking place 'by automated means.' It allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Data subjects are entitled to receive from the organisation a copy of any personal data they have provided in a 'structured, commonly used and machine-readable format,' so that they can provide the data to a different controller.

7. The right to object processing

Data subjects can object to any processing of their data that the organisation is carrying out on the lawful basis of legitimate interests. The organisation will stop processing if not able to demonstrate 'compelling legitimate grounds.'

8. Rights in relation to automated decision making and profiling

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. Profiling refers to any form of personal data processing that is

automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences, and behaviour.

The data subject has the right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling. The data subject has the right not to have decisions made about them solely by automated processing if this has a significant effect on them, unless the decision is necessary in conjunction with a contract between the data subject and the controller, or the data subject has provided explicit consent.

JMSU does not currently undertake automated decision making.

9. **The right not to receive direct marketing**

Every data subject has the right not to receive direct marketing if that is their choice.

10. **The right to claim damages in case of data breach**

If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation. See section 10 for more information about data breaches.

11. **The right to complain**

If data subjects wish to make a complaint or share concerns, they should be firstly encouraged to liaise directly with the organisation. They can make a complaint or send an email to jmsudpo@ljmu.ac.uk, who will aim to respond within 5 working days and lead on the resolution of the complaint within 28 days.

As stated in the privacy notice, we inform the data subject that they can also make a complaint to the ICO and request that the ICO carries out an assessment as to whether any of the provisions of the UK GDPR have been breached. Data subjects can remain anonymous if they wish.

18. Appendix C – Privacy & Cookies Policy

This will be found on our website below:-

- Privacy: https://www.jmsu.co.uk/privacypolicy
- Cookies: https://www.jmsu.co.uk/cookiepolicy