MISU Office and MISU Commercial Services DAC Data Protection Policy

Section 1. Policy Statement

In the course of carrying out its various functions and activities, Mary I Students' Union (MISU) collects information from staff, students, customers and other individuals in order to carry out its core functions.

The purpose of this policy is to enable Mary I Students' Union (MISU) to:

- Demonstrate its commitment to the proper handling of personal data.
- Comply with Data Protection Acts
- Protect the organisation from the consequences of any breach of its statutory and common law responsibilities.
- To encourage and support a culture of best practice in relation to data protection.

MISU is a 'data controller' under the provisions of the GDPR and the Data Protection Acts 1988-2018 and recognizes that its members have the right to know what information is held about them, and that any data held is in compliance with the GDPR and the Data Protection Acts 1988-2018. MISU processes personal information about its members and staff in accordance with the eight principles of the GDPR and the Data Protection Acts 1988-2018.

'Personal data' refers to information that identifies a living individual. MISU holds personal data for the following purposes:

1. Staff Administration – Appointments, resignations or terminations, pay, discipline, superannuation, work management or other personnel matters.
2. Administration of Advocacy/Representative/Engagement Records – details of MISU Executive Committee and Class Representatives, details of Clubs & Societies members, details of students who have obtained student-parking stickers for the relevant Academic Year, details of students who have availed of the Locker Rental system, etc.
3. Representation and Advocacy Services
4. Accounts and Records – Keeping accounts, accepting a person as a customer or supplier, keeping records of purchases, sales or other transactions, the processing of orders and accounts.
5. Advertising, Marketing and Public Relations – Advertising or marketing the business or its activities, goods or services and promoting public relations.
6. Emergency Funding– The administration of the student welfare fund.

MISU processes personal information in accordance with the eight principles of the Data Protection Act detailed in section 2.

Section 2. MISU's Conduct Statement in relation to the eight principles of Data Protection

Fair and lawful use of data

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller (MISU)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

MISU will meet this obligation in the following ways;

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, MISU will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where MISU intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of personal data will be carried out only as part of MISU's lawful activities, and MISU will
- safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to MISU and operating on its behalf in line with MISU's aims and objectives.

Be obtained only for one or more specified, legitimate purposes

MISU will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which MISU holds their data, and MISU will be able to clearly state that purpose or purposes.

Not be further processed in a manner incompatible with the specified purpose (s)

Any use of the data by MISU will be compatible with the purposes for which the data was acquired.

Be kept safe and secure.

MISU will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by MISU in its capacity as Data Controller.

Access to and management of staff, students and customer records is limited to those staff members who have appropriate authorisation and password access.

Be kept accurate, complete and up-to-date where necessary.

MISU will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. MISU conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years or as notified by a staff member.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.

MISU will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data, which is not relevant to such processing, will not be acquired or maintained.

not be kept for longer than is necessary to satisfy the specified purpose(s).

MISU has identified data categories, with reference to the appropriate data retention period for each category. This applies to data in both a manual and automated format.

Once the respective retention period has elapsed, MISU undertakes to destroy, erase or otherwise put this data beyond use.

The MISU Records Retention Schedule identifies relevant and required retention periods for data categories.

be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.

MISU has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Section 3. Staff Responsibilities

All staff who process personal data are expected to understand and adhere to the eight Data Protection Principles set out in the Acts and more specifically, the MISU Conduct Statement relating to these principles. Appropriate training will be provided, including induction training for new starters and annual refresher courses.

Significant breaches of this policy will be dealt with using disciplinary action. As such, penalties for breaching the policy must be included in contracts with third parties.

Section 4. Responsibilities of Data Subjects

Data subjects should assist MISU in ensuring that their own personal data as provided to MISU is accurate and up to date.

MISU cannot be responsible for any inaccuracies resulting directly from the submission of such information by Data Subjects nor can it be accountable for any subsequent changes to such information unless notified.

All Data Subjects have the right to review their personal information which is recorded and stored by MISU and to have it amended if necessary. All Data Subjects are entitled to be informed as to how their personal data can be kept up to date and accurate by MISU.

All staff, students and other data subjects are responsible for

- checking that any information that they provide to MISU is accurate and up to date;
- informing MISU of any changes of information, that they have provided, e.g. change of contact number
- informing MISU of any errors or changes (MISU cannot be held responsible for any errors unless previously informed).

Section 5. Sensitive Personal Data

In most cases, MISU will refrain from processing data relating to *sensitive* personal information as these matters have the potential to be used in a discriminatory way. This includes details relating to an individuals' ethnicity, religion, political opinions, health conditions, sexuality, criminal records etc. Where this is unavoidable, e.g. in the case of health and safety records, access will be limited to specific members of staff only.

Data subjects will also be required to give informed consent for MISU to use their sensitive information.

Section 6: Obtaining and Processing Personal Data

MISU obtains personal data only when there is a clear purpose for so doing and only obtains personal data, which is necessary for fulfilling that purpose. MISU ensures that this data is only used for the purpose for which it was collected.

MISU will not use its data processing facilities for capturing and storing personal data for non-business purposes.

MISU will Inform data subjects of what personal information is held and what it will be used for as well as to whom it may be disclosed.

MISU will obtain explicit consent in writing for processing sensitive data and retain a copy of that consent. Consent cannot be inferred from a non-response in the case of sensitive data.

Personal data is obtained fairly if;

- the data subject is aware of the purpose for which M I S U is collecting the data
- of the categories of person/organisation to whom the data may be disclosed
- of non-obligatory or optional answers in forms
- of the right of access to the data and of the right of rectification of the data.

Section 6.1 Disclosing Personal Data

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data is kept.

Special attention should be paid to the protection of sensitive personal data, the disclosure of which would normally require explicit written consent.

Verbal consent for the disclosure of personal data held by MISU to the data subject may be obtained by telephone in the case of non-sensitive personal data. The subject must confirm facts that should be known only to them, such as their date of birth, their student number, the reason MISU has their personal data etc. The date, time and recipient of the call should be recorded in writing.

Verbal consent for the disclosure of personal data to a third party is not permitted unless there is a statutory obligation on MISU to disclose the information. For example a disclosure to the Gardaí for the prevention of crime and where informing the subject of the disclosure would prejudice the enquiries, or unless it is in the vital interest of the data subject.

Personal data should only be disclosed to work colleagues where they have a legitimate interest in the data in order to fulfil administrative functions of MISU.

Personal data should not be disclosed outside of the EEA unless written consent has been obtained, unless disclosure is required for the performance of a contract to which the data subject is a party, or unless disclosure is necessary for the purpose of legal proceedings.

Section 6.2: Permitted disclosures of personal data

The Acts provide for disclosures of personal data, where data is:

- authorised for safeguarding the security of the State;
- required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State;
- required to protect the international relations of the State;

- required urgently to prevent damage to health or serious loss/damage to property;
- required under law;
- required for legal advice or legal proceedings;
- disclosed to the data subject;
- disclosed at the request or with the consent of the data subject.

Section 6.3 Securing personal data

MISU will protect personal data from unauthorised access when in use and in storage and such data will be protected from inadvertent destruction, amendment or corruption.
Personal electronic data should be subject to appropriate stringent controls, such as passwords, encryption, access logs, backup, etc.

Screens, printouts, documents, and files showing personal data should not be visible to unauthorised persons.

Personal manual data must be held securely in locked cabinets, locked rooms or rooms with limited access.

Subject to the MISU Records Retention Schedule, personal manual data should be destroyed by confidential shredding when the retention period has expired.

When upgrading or changing PC, ensure the hard drive is cleaned by an appropriate MIC IT staff member.

Special care must be taken where laptops and PCs containing personal data are used outside of MISU

Special care must be taken to ensure the safety and security of any personal data held on mobile storage media.

Health and social work personal data can only be released following consultation with the relevant professional.

Disclosing personal data to a Data Processor should be done only under a written contract specifying security rules to be followed.

Section 6.3: Accuracy and completeness of personal data

Administrative procedures should include review and audit facilities so that personal data are accurate, complete and kept up-to-date.

Section 6.4 : Retention of Personal Data

Data should not be kept for longer than is necessary for the purpose for which they were collected. Data already collected for a specific purpose should not be subject to further processing that is not compatible with the original purpose.

All data held by MISU should be in accordance with the Records Retention Schedule and destroyed in

accordance with that schedule and in compliance with statutory obligations.

Section 6.5: Disposal of Personal Data

Personal data should be disposed of when they are no longer needed for the effective functioning of MISU and its members. The method of disposal should be appropriate to the sensitivity of the data. Shredding is appropriate in the case of manual data and reformatting or overwriting in the case of electronic data.

Section 6.6 . Sharing Data Internally

Data is shared across business functions and between staff of MISU only when it is required in order to perform work functions. As far as possible, data is transmitted solely over a secure network and the transmission of data via paper, post or independent electronic devices is strongly discouraged.

MISU use the MIC IT network. This is a secure system which is managed by the MIC IT Department.

Section 7. Provision of Access to Third Parties

A Data Subject is entitled to access his or her own personal data only. The personal information of a Data Subject, including contact details, must not be disclosed to a third party, be they parent, potential employer, employer, professional body, sponsor, etc., without the consent of the individual concerned.

An agreement may be made to forward a communication to a Data Subject on behalf of a third party, but no information should be disclosed about the Data Subject. In the case of research surveys where there is an agreement to forward documentation to Data Subjects, a notice should be included to the effect that no personal information has been released.

Section 8. Data Subject Rights and Access Requests

Under article 15 of the GDPR, a data subject has the right to obtain a copy of any information relating to them.

GDPR provides that an individual can request access to their data free of charge and within one month of receipt of the request.

A data subject should write to MISU – contact details are outlined in Section 12 – in order to request any information, which MISU has on file relating to them. A data subject should be as specific as possible in relation to the personal data which they wish to access. MISU will require verification of a subject's identity when they make a request and the data subject should provide MISU with a copy of photo ID when making their request.

Under the normal course of events, MISU will respond to an access request within one month of receiving the

request. In certain limited circumstances, the one month period may be extended by two months – taking into account the complexity of the request and the number of requests. Where MISU is extending the period for replying to a request, MISU will inform the data subject of the extensions and the reason(s) for the delay in responding, within one month of receiving the request.

Data subjects do not have to pay a fee to make an access request. MISU will deal with a request for free however where MISU believes a request is manifestly unfounded or excessive, MISU may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s).

Exceptions to the Right of Access

Article 15 of the GDPR also provides that the right to obtain a copy of personal data must not adversely affect the rights and freedoms of others. For example, when responding to an access request, an organisation should not provide the requestor with personal data relating to a third party that would reveal the third party's identity.

Section 5 of the Data Protection Acts provides that individuals do not have a right to see information relating to them where any of the following circumstances apply.

1. If the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing / collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities

2. If granting the right of access would be likely to impair the security or the maintenance of good order in a prison or other place of detention

3. If the information is kept for certain anti-fraud functions

4. If granting the right of access would be likely to harm the international relations of the State

5. If the information concerns an estimate of damages or compensation in respect of a claim against the organisation, where granting the right of access would be likely to harm the interests of the organisation

6. If the information would be subject to legal professional privilege in court

7. If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved

8. If the information is back-up data.

Expressions of Opinion

Where personal data consists of an expression of opinion about the data subject by another person, the data subject has a right to access that opinion except if that opinion was given in confidence.

If the opinion was not given in confidence then the possible identification of the individual who gave it does not

exempt it from access.

Information about Other Individuals

Section 4(4) of the Data Protection Act makes special provision for dealing with the personal data of another individual. MISU is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure.

However, MISU is obliged to disclose as much of the information as can be supplied without identifying the other individual.

Disproportionate Effort

Section 4(9) provides that the obligation on MISU to comply with an access request, should normally be met by supplying a copy in permanent form, unless the supply of such a copy is not possible or would involve disproportionate effort.

Repeated Access Request

If MISU has complied with an access request MISU does not have to comply with an identical or similar request unless a reasonable interval has elapsed.

Section 9: Right of Rectification or Erasure

Data subjects have a right to have personal data rectified, or blocked from being processed or erased where the Data Controller has contravened the Acts.

In order to comply with this, MISU;

- Ensures that personal data is in a format, which is easy to locate and collate,
- Verifies that the access request and the personal data released refer to the same individual;
- Knows exactly what data is held on individuals, and by whom;
- Holds personal data in a secure central location.

Section 10. Data Breach

Please see the Data Breach Protocol

Section 11: Review

This policy will be reviewed from time to time to take into account changes in the law and the experience of the policy in practice

Section 12: Contact Details

General Manager
Mary I Students' Union
Mary Immaculate College
South Circular Rd
Limerick

061-400013
Deirdre.Kennelly@mic.ul.ie

Students' Union President
Mary I Students' Union
Mary Immaculate College
South Circular Rd
Limerick

061-400013
misuprez@mic.ul.ie

This document can be made available in large print upon request. If you require another alternative format please contact us to discuss your requirements.

Appendix 1 – Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, MISU refers to the definition issued by the Article 29 Working Party, and updated from time to time.)
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by MISU to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.