MAYNOOTH STUDENTS' UNION

Data Protection Policy

Contents

1. Policy Statement

1.1 Maynooth Students' Union (MSU) is a "data controller" under the provisions of the Data Protection Act 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 Data Protection Act 1988 and Data Protection (Amendment) Act 2003. MSU processes personal information about its members and staff in accordance with the eight principles of the Data Protection Act and makes sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

1.2 Complaints can lead to enforcement action being taken so it is vital that MSU has a workable and robust data protection policy that is understood and practiced across all sections of the organization.

2. Background

2.1 The **Data Protection Acts 1988 and 2003** (DPA) define a legal basis for the handling of information. It is the main piece of legislation that governs the protection of personal data in the Republic of Ireland. The Acts provides a way in which individuals can enforce the control of information about themselves.

2.2 MSU is obliged to answer any subject access requests received from individuals. These may be staff, students or any individual who has an association with MSU. They have important rights, including the right to find out what personal information is held on computer and most paper records.

2.3 To comply with the first data protection principle of the Act you have to tell individuals what their personal information will be used for, in particular:

- Who you are
- What you will use their information for; and
- Anything else necessary to make sure you are using their information fairly, including whether you plan to pass your marketing lists to other organizations and how you will be contacting people, such as by post, phone or email

2.3 Any individual with concerns about how their data may be treated is able to contact and discuss the issue with MSU.

3. Management Responsibility

3.1 The General Manager is responsible for the general development, promotion and adherence to this policy, and ultimate responsibility for compliance by all career and student staff.

3.2 The Data Protection Act 1988 & 2003 does not specify periods for the retention of personal data. It is left to staff that manage data to decide how long personal

data should be retained, taking into account the Data Protection Principles, business needs and any professional guidelines. A Data Retention Schedule has been compiled at Appendix 1.

3.3 All staff who process personal data are expected to understand and adhere to the eight Data Protection Principles set out in the Act and to ensure that they dispose of and/or destroy confidentially where necessary those records that have reached the end of their retention period. Staff should refer to the Staff Checklist for Recording Data (Appendix 2)

3.4 The General Manager is responsible for ensuring that adequate and appropriate knowledge of the Act and MSU's legal obligation is available across the organization. This is achieved by making available this policy and procedures, making training available to relevant groups, making new staff aware through their contracts of employment and working with appropriate MSU management teams to raise relevant data protection issues for discussion, resolution and to communicate lessons learnt across the organization.

4. Data Collection within MSU

4.1 Career and student staff consent to MSU using their data when they commence employment (Appendix 3). The data collected includes personal, banking, health, disciplinary and equal opportunities information. You should inform the GM of any changes to information that you have previously provided, i.e. changes of address or new information relevant to your employment

4.2 A confidential reference given to a third party for the purposes of:

4.2.1 The education, training or employment, or prospective education, training or employment, of the data subject
4.2.2 The appointment, or prospective employment of the data subject to any office, or
4.2.3 The provision, or prospective provision, by the data subject of any service

Will remain confidential, and is exempt from the subject access provisions, in that the subject cannot gain access from the person providing the reference. References should be marked confidential.

References may be accessible to the data subject if received from a third party. Your reference could become accessible from the person to whom it is sent. Care should be taken to ensure that any reference given by you is founded on fact and that viewpoints expressed can be justified.

4.3 The MSU Welfare Office has a Confidentiality Policy and their service users consent to us contacting third parties when they sign a form of authority (Appendix 4). Personal data are only ever processed in accordance with these consents.

4.4 Other MSU departments hold information in relation to its members in order to contact students with information which may be of value to them. This can be related to volunteering placements, employment placements and media contacts. Members have the option to opt-out of MSU but by joining give their consent to such information being collected. Information is also collected via our website for those joining sports teams and societies. This information

is stored on external server managed and controlled by the Maynooth University and on Google servers. Data is also collected in relation to those who are barred from MSU premises, which contains the nature of the offence which led to the barring, as well as their college and student number. Each time a customer is barred, the college security is informed.

4.5 Information relating to suppliers includes contact details, bank account details and invoices, and is stored on a secure system.

4.6 Any non-standard processing of data must be checked with the GM to ensure that it is covered by MSU's description of the processing of personal data

5. Data Sharing, Data Security and Disposal

5.1 In order to prevent unauthorized processing, or accidental loss, damage or destruction, records that hold personal data are stored in locked filing cabinets, and access to IT drives, applications and servers are managed by password only.

5.2 Data is shared across business functions and between staff of MSU only when it is required in order for them to perform their work function. Data is shared with external agencies, such as local authorities, the Gardaí upon request, and other organizations for volunteer and work placements. As far as possible data is transmitted solely over the secure network and the transmission of data via paper, post or independent electronic devices is strongly discouraged. The MSU network is a secure system with fully managed access control, back-up and recovery processes in place, managed by the Maynooth University. Google servers are used to operate email accounts for MSU and Clubs & Societies.

5.3 Where the information held on a laptop or other portable device could be used to cause an individual damage or distress, in particular where it contains financial or medical information, they will be encrypted. The level of protection provided by the encryption should be reviewed and updated periodically to ensure that it is sufficient if the device was lost or stolen; you may need to seek specialist technical advice. In addition to technical security, organizations must have policies on the appropriate use and security of portable devices and ensure their staff are properly trained in these. If it is brought to the Commissioner's attention that laptops that have been lost or stolen have not been protected with suitable encryption s/he will consider using enforcement powers.

5.4 Data is retained and disposed of according to need and in conjunction with the Data Records Retention Schedule. At the end of the retention period data are disposed of and/or destroyed, confidentially where necessary. Manual files are shredded and electronic data is deleted from central systems.

6. Sharing Data Routinely with Other Organizations

6.1 MSU has no responsibility for the management of personal data processed by the Maynooth University, which is solely responsible for its own compliance with the Act. The Maynooth University provides a separate notification to the Data Protection Commissioner and is responsible for responding to requests for access to information in its possession.

6.2 MSU reserves the right to share information with Maynooth University as necessary to pursue its legitimate interests, or to ensure the smooth operation of procedures and practices in the interests of students, staff and other individuals connected to MSU. Disclosure of personal data is always made in accordance with the Data Protection Act and never prejudices an individual's rights or freedoms.

6.3 Under circumstances relating to disciplinary activity both MSU and the Maynooth University reserve the right to pass necessary information (including personal data) to the other in order to uphold and enforce disciplinary procedures.

6.4 Both MSU and Maynooth University have varying degrees of responsibility for areas of the campus designated for social use. When an individual is banned from such areas, it is in the legitimate interests of both MSU and the Maynooth University to communicate and pass on relevant information to ensure the ban is implemented successfully. In order to ensure disciplinary procedures are upheld and enforced, personal data relating to individual subjects to disciplinary action or related enquiries may be passed between them.

7. Requests for Information

7.1 In order to fulfil their responsibilities under the act the organization may, before responding to any request, seek proof of the requestor's identity and any further information required to locate the personal data requested.

7.2 On receipt of a request all Department Heads will automatically be asked to supply copies of any data concerning the individual which they hold.

7.2 Individuals have the right to request what personal information is held about them on computer and can get access to most paper records. The Data Protection Act gives you the right, as a "data subject", on payment of an "access fee" to receive details of all personal information which concerns you and which is stored and processed by MSU. Requests for such information should be made by completing the form attached at Appendix 6 and forwarding it to the General Manager. It should be accompanied by a cheque, made payable to MSU, in payment of the access fee, which currently stands at €20. The Data Protection Act requires MSU to provide information to you within 40 days.

8. Complaints

8.1 Individuals concerned about any aspect of the management of personal data at MSU are able to raise their concerns in a fair and equal way. Complaints can be registered with the General Manager. If an individual is not satisfied that their complaint has been properly dealt with they should contact the Chair of the MSU Board of Trustee's.

8.2 If an individual feels they are being denied access to personal information they are entitled to, or feel that their information has not been handled according to the eight principles, they can contact the
Office of the Data Protection Commissioner.
Canal House, Station Road, Portarlington, Co. Laois, Ireland.
LoCall 1890 25 22 31 | Phone 00353 57 868 4800 | Fax 00353 57 868 4757 |
email info@dataprotection.ie

APPENDIX (A) – DATA RETENTION SCHEDULE

General Administration **1. Staff/Personnel Records – Personnel Office**	
Records	**Recommended Retention Period**
	If under appeal or if litigation is likely hold in original form indefinitely, otherwise retain records for the minimum periods set out below.
Unsolicited applications for	Hold for six months and then destroy.
Applications for a vacant post Candidates not short-listed. Candidates short-listed but not	Hold for 1 year.
General Job Description file It is recommended that the job description be filed on the personal file of the successful	Hold until superseded.
Recruitment Competitions Vacancy notification. Advert Copies.	Retain indefinitely.
Applications & Curriculum Vitae of candidates who are called for interview. Selection Criteria. Applications & Curriculum Vitae of Candidates not qualified or short-listed. Interview Board Marking Sheet/Report. Interviewers' notes Establishment of Panel	 Hold for one year. Retain indefinitely. Destroy once marking sheet has been completed. Hold for one year.
Staff Personnel Files Applications and Curriculum Vitae of candidates who are offered and take up a post, together with the following (where applicable): Advertiseme nt Copy References. Recruitment Medical. Employment Records. Offer/Acceptance of Appointment. Contract of employment/Job specification. Calculations relating to incremental credit and point on scale at appointment. Job share record.	Retain for duration of employment. On retirement or resignation, hold for six years, but retain service record indefinitely. Destroy remainder (see disciplinary records for exceptions). Retain indefinitely

General Administration 2. Financial Records	
Records	**Recommended Retention Period**
	If under investigation or if litigation is likely hold in original form indefinitely otherwise retain records for the minimum periods set out below
Accounts Payable	
Batches of Invoices and Vouchers	Hold in original form for 6 years.
VAT Records	Hold hard copy for 6 years, unless otherwise authorised by Revenue Commissioner
Tax Clearance Certs	Hold until audit signed off and superseded
Accounts Receivable	
Debtors Ledger	Hold for 6 years
Income Listings	Hold for 6 years
Income Control Accounts	Hold for 6 years
Receipts Reconciliation	Hold for 6 years
Agreements - Rental, Lease, Use, Occupancy	Retain indefinitely
Bank Records	
Paid Cheques	Hold until audit signed off
Bank Reconciliations	Hold until audit signed off
Bank Statements	Hold until audit signed off
Capital Projects	Hold for seven years after completion and destroy
Financial Statements	
Annual Financial Statements	Retain indefinitely in original form
Final Budgetary reports/estimates for any year	Retain indefinitely in original form
Registers maintained in Finance Department under statute i.e. Reg. of insurances, mortgages assets	Retain indefinitely in original form
Fixed Assets	
Records of Boards Properties, Sale and Purchase	Retain indefinitely in original form
Assets Register	Retain indefinitely in original form
Insurance Files	
Policies	Hold indefinitely
Accident reports	6 years following settlement
Claims correspondence	6 years following settlement
Other Records	
Audit Reports	Permanent
Financial Regulations, Policies and Accounting Standards, Accounting Legislation, Monthly Expenditure and Income Reports	Hold until superseded or audit signed off, whichever is later.
Travel/Expense Claims	6 years
Receipt Books	6 years
Purchase Order Books	6 years
Cash Payments/receipts	6 years
Petty Cash	6 years
Correspondence on financial administration	6 years

Supplier records	6 years
Tender documentation	6 years
Payroll	
Payslips	6 years
Pay sheets Authorisations to deduct, tax details of staff, appointment details, pay scales	Hold in original form for six years.

General Administration 3. Legal Records	
Records	**Recommended Retention Period**
Contracts for Services	6 years after expiration of contract
Commercial Contracts	6 years after expiration of contract
Legal cases	Permanent
Legal opinion/correspondence	Permanent
Copyright/trademark registration	Permanent
Data Protection registrations	Permanent

General Administration 4. Committee Records including minutes/reports/supporting documentation	
Records	**Recommended Retention Period**
Executive	Permanent
Union Council	Permanent
Other Sub-Committees	Permanent
Senate	Permanent
Board of Trustees	Permanent
	Permanent
	Permanent
Departmental Meetings	Permanent
Programme Design Teams	Permanent
Steering Committees	Permanent
Hand written notes taken by recording secretary at meetings	Destroy once minutes of the relevant meeting have been agreed
Numerous other Committee /meeting records operate within Clubs & Societies	Hold until no longer considered relevant.

General Administration 5. Health & Safety Records	
Records	**Recommended Retention Period**
College Safety Statements	Hold until superseded
Safety Records	10 years
Accident Reports	10 years
Fire inspection records	6 years
Safety training records	Lifetime of employee
Catering inspection records	5 years
Risk Assessment	5 years

General Administration 6. Other	
Records	**Recommended Retention Period**
General Correspondence, including e-mails	Hold until no longer considered relevant
Statistics	Depends on context in which they were gathered
Membership information, including society/sports/ volunteers/media	3 years
Casework	1 year

APPENDIX (B) – STAFF CHECKLIST FOR RECORDING DATA

	Yes (✓) No (X)
1. Do you really need to record the information (i.e. is this the only method of making the information readily available)	
2. Is the information standard (✓) or is it sensitive (X)	
3. If it is sensitive, do you have the data subject's express consent?	
4. Has the data subject been told that this type of data will be processed?	
5. Are you authorised to collect/store/process the data? **If Yes, have you checked with the data subject that the data is accurate?**	
6. Are you sure that the data is secure?	

APPENDIX (C) – DATA COLLECTION FROM STAFF

Excerpt from the Terms and Conditions of Employment

I accept the terms of this offer and agree to abide by them. I also understand that from time to time MSU may wish to process any personal information (as periodically updated) contained within this document for personnel administration and business management purposes. I understand that where this is the case, processing will take place in accordance with the provisions of the Data Protection Acts 1988 and 2003. By signing this form I acknowledge that I will be providing the company with my consent to these uses.

FULL NAME:……

SIGNATURE …… DATE:

APPENDIX (D) – FORM OF AUTHORITY FOR WELFARE SUPPORT

Maynooth Students' Union
North Campus, Maynooth University
Maynooth County Kildare
Telephone (01) 708 3669

To whom it may concern

I hereby authorise the appropriate MSU Staff and Officers to undertake casework on my behalf, and to communicate with staff of Maynooth University for this purpose.

The following staff should not be contacted:

.....

This includes verbal, written and electronic communications.

Name:.....

Course and year:…….....

Course dates:.....

Student status: Current Leave of absence Completed

Signed:.....

Date: .....

APPENDIX (E) - DATA SUBJECT ACCESS REQUEST FORM FOR STUDENTS AND STAFF

I,_____wish to have access to data which Maynooth Students' Union has about me in the following categories: (Please tick as appropriate.)

□ Employment references

□ Disciplinary grievance and capability records

□ Health and medical matters

□ Political, religious or trade union information

□ Any statements of opinion about my abilities or performance

□ Personal details including name, address, date of birth etc

□ Other information: please list below

_____

_____

_____

_____

Signed _____

Date _____