DITSU Policy on Data Protection

Contents

Policy Statement

While carrying out its various functions and activities, DIT Students' Union (DITSU) collects information from individuals and external organisations and generates a wide range of data which is recorded and maintained. The purpose of this policy is to enable DITSU to:

- Demonstrate its commitment to the proper handling of personal data
- Comply with Data Protection law
- Protect the organisation from the consequences of any breach of its statutory and common law responsibilities
- Encourage and support a culture of best practise within data protection.

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

- Staff Administration – appointments/removals, pay, discipline, work management and other personnel matters.
- Accounts and Records – keeping accounts, records of customers and suppliers, records of purchases or other transactions, the processing of orders and accounts.
- Administration of member records, including elected representatives and volunteers
- Casework – student contact and demographic details relating to education and welfare matters that DITSU has been requested to advise and advocate on.
- Fundraising – fundraising in support of the chosen RAG Charity.

DITSU processes personal information about its members in accordance with the principles of the General Data Protection Regulation (GDPR) detailed below:

Principle 1 - Lawfulness, Fairness and Transparency
Transparency: Tell the subject what data processing will be done.
Fair: What is processed must match up with how it has been described
Lawful: Processing must meet the tests described in GDPR

Principle 2 - Purpose Limitations
Personal data can only be obtained for "specified, explicit and legitimate purposes". Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

Principle 3 - Data Minimisation
Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". i.e. No more than the minimum amount of data should be kept for specific processing.

Principle 4 - Accuracy
Data must be "accurate and where necessary kept up to date". Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

Principle 5 - Storage Limitations
Regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary”. i.e. Data no longer required should be removed.

Principle 6 - Integrity and Confidentiality
Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage”.

DITSU respects individuals right to privacy and will not collect any personal information digitally or elsewhere, without the express permission of that individual. Any personal information which is volunteered will be treated with the highest standards of security and confidentiality, strictly in accordance with Data Protection Regulation.

What this Means for me?

As a DITSU Staff Member
Staff members must be cognisant of upholding this policy and adhere to the General Data Protection Regulation whilst processing any data as set out below. Staff members who breach this policy will be answerable to the CEO and may be subject to HR procedures.

Staff members will be given training on handling data, and any clarifications will be addressed by the Data Controller in the first instance followed by the Board of DITSU CLG.

As a DITSU Elected Officer
DITSU Officers must be cognisant of upholding this policy and adhere to the General Data Protection Regulation whilst holding any data as set out below, Staff members are generally the data processors, and any data collection should be sign-posted or pass directly to the appropriate person. Officers who breach this policy will be answerable to the CEO and may be subject to HR procedures.

Elected Officers will be given training on handling data, and any clarifications will be addressed by the Data Controller in the first instance followed by the Board of DITSU CLG

As a DIT Student
DITSU endeavours to protect the rights of all students it holds data on – both with regard to the retention and disposal of data, as well as providing the means for students to request access to any information held on them.

As a Third Party to DITSU
DITSU endeavours to protect the rights of third party stakeholders it holds data on – both with regard to the retention and disposal of data, as well as providing the means for stakeholders to request access to any information held on them.

Background

The Irish Data Protection Acts 1998 and 2003 were replaced by the European wide General Data Protection Regulation (GDPR) on the 25th May 2018 and defines the legal basis for the processing of personal information relating to living individuals. GDPR protects European Union data subjects' fundamental right to privacy and the protection of personal data. It introduces robust requirements that raise and harmonise standards for data protection, security, and compliance.

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

Under the GDPR, when personal data is collected from data subjects, DITSU must provide the following information:

- Identity and contact details of DITSU
- Contact details for the Data Controller
- Purpose of the intended processing and its legal basis
- If the legal basis is a “legitimate interest” of DITSU, what that interest is
- The intended recipients of the data
- Any intention to transfer the data outside the EU and if so, data safeguards in that country
- The period for which the data will be stored or the basis for determining that period
- The data subjects right to request access, rectification, erasure, restriction of use, objection of use and data portability
- The data subjects right to lodge a complaint to a supervisory authority
- Whether DITSU must provide data as part of a statutory or contractual requirement and the consequences of not providing the data
- The existence and logic of any automated decision making or profiling processes

If DITSU intends to process data for a purpose other than the purpose for which it was collected, the controller must provide the data subject with information about this purpose before processing begins.

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

1. Management and Staff Responsibilities

1.1 The Chief Executive Officer is responsible for the general development, promotion and adherence to this policy, and ultimate responsibility for compliance by all staff.

1.2 GDPR does not specify periods for retention. DITSU has agreed upon a set of retention periods as laid out in the Data Records Retention Schedule **(Appendix 1)**

1.3 All staff who process personal data are expected to understand and adhere to the Data Protection Principles and ensure that they dispose of and/or destroy, confidentially where necessary, records that have reached the end of their retention period.

1.4 The Chief Executive is responsible for ensuring that adequate and appropriate knowledge of the GDPR and DITSU's legal obligation is available across the organisation. This is achieved by making available this policy and procedures, training relevant employees and making new staff aware through their contracts of employment.

2. Student Responsibilities

2.1 Students should assist DITSU in ensuring that their own personal data as provided to the Union is accurate and up to date.

2.2 Students volunteering for DITSU[1] may need to process personal data for activity administration purposes. If students are using personal data, they must inform the relevant DITSU staff member in charge of the activity so that the requirements of the GDPR can be adhered to.

3. Data Collection within the Union

3.1 Staff consent to the Union using their data when they commence employment. Staff must inform HR of any changes to information that have previously been provided.

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

3.2.1 The education, training or employment, or prospective education, training or employment, of the data subject
3.2.2 The appointment, or prospective employment of the data subject to any office
3.2.3 The provision, or prospective provision, by the data subject of any service.

will remain confidential and is exempt from 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. The reference could become accessible from the person to whom it is sent. Care should be taken to ensure that any reference given by DITSU is founded on fact and that viewpoints expressed can be justified.

[1] i.e. Elected democratic positions, ents crew, welfare crew etc.

3.3 DITSU's Education and Welfare Service has an Education and Welfare Charter and students consent to the Union contacting third parties when they sign a form of authority **(Appendix 2)**. Personal data will only be processed in accordance with these consents.

3.4 In most cases DITSU 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. In circumstances where this information is required for the data processing purpose, access will be limited to specific members of staff only. Data subjects will also be required to give informed consent to DITSU to use their sensitive information.

4. Data Sharing, Data Security and Disposal

4.1 To prevent unauthorised processing, or accidental loss, damage or destruction, records that hold personal data are stored in locked cabinets, and access to IT drives, applications and servers is managed by password only.

4.2 Data is shared across business functions and between staff of DITSU only when it is required for them to perform their work function. Data is shared with external agencies, such as government authorities e.g. the Gardaí upon request. 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.

4.3 All laptops and portable devices used by DITSU must be encrypted. The level of protection provided should be reviewed and updated periodically, in conjunction with the IT provider to ensure that it is sufficient if the device was lost or stolen. Please refer to the **Company Devices User Policy**.

4.4 Data is retained and disposed of according to need and in conjunction with the Data Records Retention Schedule **(Appendix 1)**. At the end of the retention period data is disposed of and/or destroyed, confidentially where necessary. Manual files are shredded, and electronic data is deleted from local and central systems.

4.5 A third party 'Memberships Solutions Limited ('MSL') will provide an information management system to link in with the Dublin Institute of Technology's (DIT) student record system – personal data of students will not be directly accessible by DITSU. MSL are bound by a contract stating that personal information will not be modified, deleted, or shared, without the instructions of DITSU, or used for any purpose other than that specified by DITSU. They are also contractually obliged to abide by GDPR. Where the system provider changes, any future provider will be added to this policy. For further information, please see the **Website User Policy.**

5. Sharing Data Routinely with Other Individuals and Organisations

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

5.2 DITSU reserves the right to share information with DIT 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 the Union.

5.3 Disclosure of personal data is always made in accordance with the principles of the GDPR and never prejudice an individual's rights or freedoms.

5.4 In the case of personal information requests by the Gardaí or government authority for the purposes of the prevention or detection of crime or for taxation, and where it is not appropriate for the requestor to seek that information from the individual(s) concerned, it may be deemed necessary to release personal data to the third party. The GDPR allows for a data controller to release personal data for:

- The prevention or detection of crime
- The apprehension or prosecution of an offender
- The assessment or collection of tax or duty or of any imposition of a similar nature.

Unless a Court order is made, the decision regarding whether to release personal data will belong to DITSU.

6. Request for Information, erasure and modification

6.1 Data subjects have the right to see a copy of any personal data held by DITSU about them, and they can request this information free of charge. DITSU must respond to them within one month, but this can be extended for a further two months if the information sought is of a complex nature

They are entitled to the following information:

- The purposes of the processing
- The categories of data being held
- The identity of any recipients who may see this data
- The period for which it will be stored
- The right to lodge a complaint with a supervisory authority
- Where the information was not collected directly from them, information about the source
- The use of any automated decision-making processing and information about that process
- If data is being transferred to a country outside the EU, the data safeguards in that country apply.

6.2 To fulfil the responsibilities under the act DITSU may, before responding to any request, seek proof of the requestor's identity and any further information required to locate the personal data requested.

6.3 On receipt of a request DITSU's Management Team will automatically be asked to supply copies of any data concerning the individual which they hold.

6.4 Individuals have the right to request what personal information is held about them on computer and can get access to most paper records. The GDPR gives the Data Subject the right of access to receive details of all personal information which concerns them, and which is stored and processed by DITSU. Request for such information should be made by completing the attached form **(Appendix 3)** and forwarding it to the CEO.

6.5 Any information requested must be supplied to the individual within 30 days of receiving a formal request.

6.6 Data subjects can request and receive personal data that they have previously provided to DITSU in a commonly used and machine-readable format. The right also means they can request DITSU to transfer their personal data to another controller.

6.7 If a data subject wishes any of their personal information held by DITSU to be blocked, erased or destroyed they should email mydata@ditsu.ie In some cases (i.e. records relating to a criminal investigation) there may be legitimate reasons for DITSU to preserve personal information.

6.8 As a Students' Union, DITSU is not a "public authority" in the sense of the Freedom of Information (FoI) Act. This means that records of DITSU itself will not be covered by Freedom of Information and cannot be requested under FoI.

6.9 Data subjects have the right to request that DITSU rectifies inaccurate or incomplete personal data held on them.

Data subjects have a right to restrict DITSU from processing their personal data where:

- The accuracy of the data is in question
- The processing of the data is unlawful
- DITSU no longer needs the data for the purpose, but it is required by the data subject for other reasons
- Data subjects have challenged the legal basis for the processing

6.10 Once processing has been restricted, DITSU must inform the data subject before that restriction is lifted. The data subject can request DITSU to erase their data, and DITSU has an obligation to erase that data if one of the following applies:

- The data is no longer necessary for the purpose it was collected
- The data subject has withdrawn consent to the processing of their data
- The data subject objects to the processing of their data
- There is no lawful basis for the processing
- The data must be erased to comply with law
- The data was collected in relation to the offer of online services

6.11 The right of erasure also includes the right to have publicly available personal data erased or as far as technologically possible, removed from public availability. The GDPR also gives legislative effect to the 'right to be forgotten' procedure. Right to be forgotten is a right to have search engine results that relate to a person, or a certain incident, removed from internet search listings once that information is no longer

relevant. For example, if an online search for your name turned up a link to a photograph of a person that they believe is no longer relevant for the purpose for which it was collected, they can request that the search engine remove that link from their search results. The right to be forgotten is not an absolute right and requests under the procedure are assessed on a case-by-case basis.

6.12 The right of erasure will not apply where processing is necessary because of an overriding freedom of expression, legal or public interest.

7. Marketing and Communications

7.1 Data subjects have the right to object to the processing of their data at any time, for example to prevent data being used for marketing purposes, including profiling.

7.2 If students would like to be removed from a mailing list, they may opt out of that type of communication by replying to the sender or emailing mydata@ditsu.ie Communications will not contain information that would not be reasonably expected, given the relationship between students and DITSU.

8. Collection and use of technical information

The DITSU website may use cookies. Visitors can use this website with no loss of functionality if cookies are disabled from the web browser. Technical details in connection with visits to the website may be logged for statistical purposes. The technical details logged are confined to the following items:

- The IP address of the visitor's web server
- The top-level domain name used (for example .ie, .com, .org, .net)
- The previous website address from which the visitor reached us, including any search terms used
- Clickstream data which shows the traffic of visitors around this web site (for example pages accessed and documents downloaded)
- The type of web browser used by the website visitor.

9. Data Breach

According to the General Data Protection Regulation appropriate security of personal data is required, including protection against unlawful processing and against accidental loss or damage. In the unlikely event of a data breach, staff must inform the Data Controller – please see **Appendix 2.**

DITSU must notify the Data Controller of a personal data breach without delay where that breach is a likely to result in a risk to the rights and freedoms of the data subject. Notification should be made within 72 hours of DITSU becoming aware of the breach. Staff are required to notify DITSU if they become aware of a breach. DITSU should also notify the data subject without delay.

In the case of a serious breach occurring, the Data Controller must inform the Office of the Data Protection Commissioner.

10. Complaints

Individuals concerned about any aspect of the management of personal data in DITSU can raise their concerns in a fair and equal way. Complaints can be registered in writing or by email with the Data Controller. If an individual is not satisfied that their complaint has been properly dealt with they should contact the Chair of the Board of DITSU CLG.

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 six principles, they can contact the Office of the Data Protection Commissioner:

Telephone	+353 (0) 57 868 4800 +353 (0) 76 110 4800
Lo Call Number	1890 252 231
E-mail	info@dataprotection.ie
Postal Address	Data Protection Commission Canal House Station Road Portarlington R32 AP23 Co. Laois

Appendix 1 - Data Records Retention Schedule

Description of Data	Retention Period	Reason/Authority for Retention Period	Erasure Action
Staff application forms, Interview notes (unsuccessful applicants)	12 months from the date of interviews	Limitation period for litigation	Shred hard copy files Delete data files
Employee's terms and conditions of employment	Retained for the duration of employment	Terms of Employment (Information) Act, 1994	Shred hard copy files Delete data files
Payslips showing the employees were paid at least minimum wage.	3-year retention period	National Minimum Wage Act, 2000	Shred hard copy files Delete data files
Employees weekly working hours, the name and address of employee, the employee's PPS numbers and a statement of their duties.	3-year retention period	Organisation of Working Time Act, 1997, Organisation of Working Time (Records) (Prescribed Form and Exemptions) Regulations 2001	Shred hard copy files Delete data files
Tax and Accounting Records	6-year retention period	Companies Acts and Taxes Consolidation Act, 1997	Shred hard copy files Delete data files
Accident in the Workplace	10-year retention period	The Safety, Health and Welfare at Work (General Applications) Regulations 1993	Shred hard copy files Delete data files
Facts relating to redundancies	3 years from date of redundancy	Collective redundancy information	Shred hard copy files Delete data files
Statutory Maternity and Paternity Pay records and calculations	8 years after the end of the financial year to which the records relate	Maternity Protection Act, 1994 Paternity Leave and Benefit Bill, 2016 Parental Leave Acts 1998-2006	Shred hard copy files Delete data files

Description of Data	Retention Period	Reason/Authority for Retention Period	Erasure Action
Wages and salary records	6 years from the last date of employment (7 is advisable)	Code of Practice for Revenue Audit and other Compliance Interventions	Shred hard copy files Delete data files
Suppliers	7 years after the end of the financial year to which the records relate		Shred hard copy files Delete data files
Board Meeting documents i.e. agendas, minutes etc	6 year retention period	As per Companies Act 2014	Shred hard copy files Delete data files
Data Base of Directors and Members	6 year retention period	As per Companies Act 2014	Shred hard copy files Delete data files
Membership information, including: Elected Representatives, Volunteers	Up to 3 years from the date of membership		Shred hard copy files Delete data files
Casework	1 full academic year following date of entry (to 30th June 20XX)		Shred hard copy files Delete data files
Democratic Databases	1 full academic year following date of entry (to 30th June 20XX)		Shred hard copy files Delete data files
Emails	3 years, with exceptions.		Delete data files
Passwords on all electronic devices	Every 6 months		

Appendix 2 - Data Breaches under GDPR

According to the GDPR a personal data breach is considered to be: *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored, or otherwise processed".*

If a personal data breach occurs the individuals concerned must be informed of the breach by the Data Controller, and if the breach is deemed to be of medium to severe risk, the GDPR has introduced a requirement to notify the Data Protection Commissioner.

Types of Data Breaches

Broadly speaking, breaches can be classified into 3 areas:

- **Confidentiality breach** – where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **Integrity breach** – where there is an unauthorised or accidental alteration of personal data.
- **Availability breach** – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Risk areas affecting DITSU which have been identified include:

- Sharing of personal email addresses by not using the "bcc" line
- Sharing of data without obtaining permission from the individual
- Alteration of data without permission of the individual
- Not deleting data when requested to do so by an individual
- Not disposing of data in the required manner under the Data Protection Policy, within the required timeframe
- Unauthorised removal of Data from DITSU premises
- Loss or theft of devices containing data

Levels of risk can be classified as follows:

- Low Risk - The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal
- Medium Risk - The breach may have an impact on individuals, but the impact is unlikely to be substantial
- High Risk - The breach may have a considerable impact on affected individuals
- Severe Risk - The breach may have a critical, extensive or dangerous impact on affected individuals.

What happens when a Breach has occurred?

1. The Data Controller must be informed as soon as a breach occurs
2. The Data Controller will enter the details into the DITSU Data Protection Breach Register
3. The Data Controller will consider the likely consequences of the breach and give it a risk rating.

4. The Individual/s concerned will be contacted (if the breach is determined to be of medium to severe risk) and informed of the breach, advised on the action DITSU will be taking and whether any mitigating processes will be put in place and also advised on their rights under Data Protection Regulation.
5. If the breach is deemed to be of medium to severe risk, the Office of the Data Protection Commissioner will be informed via a “Breach Notification” form. This must be done within 72 hours of the Data Controller becoming aware of the breach.
6. If deemed appropriate, the staff member/officer will be given additional training

Appendix 3 - Glossary of Terms

Company Devices User Policy
A DITSU policy which outlines the use of mobile devices used by DITSU employees and full-time officers.

Data Controller
The Data Controller has the most responsibility when it comes to protecting the privacy and rights of the data's subject, such as the user of a website. They control the procedures and purpose of data usage.

In DITSU the Data Controller is Claire Healey.

Data Processor
A data processor processes any data that the data controller gives them. The data processor does not own the data that they process, nor do they control it. This means that the data processor will not be able to change the purpose and the means in which the data is used. Furthermore, data processors are bound by the instructions given by the data controller.

Data Protection Commissioner
The Data Protection Commissioner is appointed by the Government. The Commissioner is independent in the exercise of their functions. Individuals who feel their rights are being infringed can complain to the Commissioner, who has powers to enforce the provisions of the Act.

DITSU Education and Welfare Service
Service offered by DITSU providing information, guidance and representation for members in relation to education and welfare issues. The Education and Welfare Charter available from DITSU sets out details of this service.

GDPR
EU 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Sensitive Personal Information
Information about a data subject, which goes beyond contact information and identifying documentation. Areas which are considered sensitive include: religion, ethnicity, sexual orientation, trade union membership, medical information etc. Sensitive personal information is handled in a more stringent manner.

Website User Policy
The DITSU website is run by a third party - Memberships Solutions Limited ('MSL'). They provide an information management system to link in with the DIT student record system – personal data of students will not be directly accessible by DITSU. MSL are bound by a contract stating that personal information will not be modified, deleted, or shared, without the instructions of DITSU, or used for any purpose other than that specified by DITSU.

Appendix 4 - Consent Forms for DITSU Advice Service

4.1 DITSU Confidentiality/Data Protection Statement

The DITSU Education and Welfare Charter ensures that anything you discuss with a DITSU member of staff will not be disclosed without your permission or consent, however, there are two instances where confidentiality cannot be promised.

1. In the first instance if we have reason to believe that you (if under the age of 18), or any child under 18 in your care, is being abused or neglected. We are mandated, which means that we are legally obligated under the 1991 Child Care Act, to make a report to the Child Protective Services (TUSLA).

2. The second instance where we would have to break confidentiality, is if you made a serious threat to harm yourself, or someone else. By "serious threat" we mean a situation where you said something that led us to believe you truly intended to harm yourself, or another person. We would disclose that to the appropriate persons to keep you safe. If another person was at risk, we would need to warn that person, or the appropriate authorities. Again, if we need to break confidentiality regarding something you have disclosed, we will discuss this with you first.

DITSU are legally bound to uphold the Data protection laws in Ireland and you can also view your rights regarding Data protection

DITSU respects your right to privacy and will not collect any personal information about you on the website or elsewhere, without your express permission. Any personal information which you volunteer will be treated with the highest standards of security and confidentiality, strictly in accordance with the EU General Data Protection Regulation (GDPR)

4.2 Consent Form for Students Accessing DITSU Advice Service (Hard Copy)

To whom it may concern within the DITSU Education and Welfare Advice service

1. I hereby authorise the appropriate DITSU Staff to undertake casework on my behalf and to communicate with relevant staff of the Dublin Institute of Technology and any other appropriate third parties*, for the purposes of addressing my query.

2. I understand that any data which I voluntarily disclose, will be held on file for a period of one full academic year following date of entry (to 30th June 20XX) - after which it shall be deleted and destroyed. Or at any time I may request that my data is updated or deleted.

3. I give my consent that DITSU can use my contact details as noted below as part of my Casework.

Name: ……..

Email Address: ……...

Phone Number……..……

Student Number…….

Programme/Year: …….

Signed: ……

Date: ……

** Secondary permission may be required in certain circumstances.*

DITSU endeavours to protect the rights of all students it holds data on – both with regard to the retention of and disposal of such data, as well as providing the means for students to request access to any information held on them. For further information on how DITSU processes your data, please refer to the DITSU Policy on Data Protection or email mydata@ditsu.ie.

4.3 Consent Form for Students Accessing DITSU Advice Service (Soft Copy)

Subject Line: Do you agree to the DITSU Data Protection Statement?

Dear **(NAME),**

Thank you for contacting us with your query.

Your reference # for this case is: **(NUMBER).** The subject of your case is: **(TITLE)**

In order for us to proceed with this case we need you to reply to this email. Stating that you agree to the DITSU Data Protection Statement below and give your consent;

To whom it may concern within the DITSU Education & Welfare Advice service

1. I hereby authorise the appropriate DITSU Staff to undertake casework on my behalf and to communicate with relevant staff of the Dublin Institute of Technology and any other appropriate third parties*, for the purposes of addressing my query.

2. I understand that any data which I voluntarily disclose, will be held on file for a period of one full academic year following date of entry (to 30th June 20XX) - after which it shall be deleted and destroyed. Or at any time I may request that my data is updated or deleted.

3. I give my consent that DITSU can use my contact details given (email/phone number) as noted in this email as part of my case file.

* Secondary permission may be required in certain circumstances.

DITSU endeavours to protect the rights of all students it holds data on – both with regard to the retention of and disposal of such data, as well as providing the means for students to request access to any information held on them. For further information on how DITSU processes your data, please refer to the DITSU Policy on Data Protection or email mydata@ditsu.ie

Appendix 5 - Data Access Request Form

I wish to make a data access request pursuant to Article 15 of the General Data Protection Regulation (GDPR) and, or section 91 of the Data Protection Act 2018. (This form can also be found online)

Section 1 – Your Details

Surname	
First Name (s)	
Previously known as (if applicable)	
Current Address	
Prior Address (if applicable)	
Contact Phone Number	
Contact Email Address	

Section 2 – Your relationship with DIT Students' Union

Please describe in as much detail the nature of your relationship with DITSU. Relevant points could include: • Were you a staff member, full/part time elected representative, student • Staff or student number • Beginning and end dates of your relationship with DITSU • If a student, which area of DITSU your relationship covered – i.e. democracy, events etc.	

Section 3 – Details of Personal Data Requested

Please describe, in as much detail as you can, the nature of the personal data requested. It is not sufficient to ask for 'everything about me'. If your request is too broad or unclear we may need to ask you to be more specific. Possible points to consider are: • Description of the personal data held • Likely location • Any identifying references numbers, codes etc. • Likely dates of when the personal data was created.	

Section 4 – Identification

To process your application in accordance with best practice it is necessary for you to provide proof of your identity. Possible forms of ID accepted are: • A recent utility bill (must be less than 6 months old at the time of application) • Passport (page with your signature) • Driving Licence (page with your signature) • University Student ID Card • Garda Age Card

Section 5 – Agent Details (if applicable)

If you wish to appoint an agent (e.g. a family member, friend, solicitor) to act on your behalf in connection with your personal data access request please complete this section.	
I confirm that I wish to appoint the individual named below to act on my behalf in relation to the personal data access request which is the subject of this form.	
Agents Name	
Agents Address	
Agents Contact Phone Number	
Agents Email Address	
Relationship of agent to me	

Section 6 – Declaration

I confirm that I am the data subject named in section 1 above. In accordance with Article 15 of the General Data Protection Regulation, I request a copy of the personal data held on me by DIT Students' Union. I also confirm that the details set out by me on this application form are, to the best of my knowledge, true and accurate.	
Signed	
Date	

Please hand in form to one of the Union offices, or post the form to

Data Protection Office
DIT Students' Union
DIT Bolton Street
Dublin 1