

GDPR – Subject Access Request Policy

Version 1

Document Location

Data Protection Office

Revision History

Date of drafting: April 2019	Date of next review: April 2022
------------------------------	---------------------------------

Version Number/Revision Number	Revision Date	Summary of Changes
V 1.0	--	--

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
	11 June 2019	Finance Audit Risk Committee	--

Approval

This document requires the following approvals:

Name	Title	Date
Governing Body		23 Sept 2019

This Policy was agreed by the Governing Body on 23 September 2019. It shall be reviewed and, as necessary, amended by the Institute every three years. All amendments shall be recorded on the revision history section above.

Table of Contents

Page No:

1. Introduction	4
2. Purpose	4
3. Definitions	5
4. Scope	5
5. Roles and Responsibilities	5
5.1 Roles GDPR – Subject Access Request Policy	5
6. Receiving Requests	5
7. Fees	6
8. Timescales	7
9. Locating Requested Information	7
10. Screening Information	8
11. Providing Information	8
12. Data Processors and Subject Access Requests	8
13. Monitoring of Subject Access Requests Responses	9
14. Policy Review	9
15. Appendix A – List of Policies and Procedures to be read in tandem with this policy	10

1 Introduction

1.1 Article 15 of the General Data Protection Regulations (GDPR) provides individuals (known as Data Subjects) with the right to access personal information so that they are fully informed of the nature of any processing and to verify the lawfulness of the Institute's processing of their personal data.

1.2 The right allows them to obtain confirmation as to whether personal data is being processed by the Institute, and where it is being processed, so they are entitled to access the following information:

- A copy of the data (subject to any exemptions)
- The reasons why their data is being processed.
- The description of the personal data concerning them.
- Anyone who has received or will receive their personal data.
- Details of the origin of their data if it was not collected from them directly.

1.3 This right of access extends to all information held about the Data Subject, for example personnel files, student files, interview notes and emails that refer to them.

1.4 Data Subjects requesting their information must submit a Subject Access Request (SAR) to the Institute which outlines what information they wish to receive and proof of their entitlement to access it (Proof of identity such as a Student Card, passport or driving licence).

1.5 Under the General Data Protection Regulations, some personal data is exempt from disclosure if disclosing it would 'adversely affect the rights and freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software.'

1.6 The Irish Data Protection Act introduces further exemptions to SARs such as those for national security, defence, law enforcement and public security.

1.7 The Policy sets out the manner by which the Institute will respond to Subject Access Requests.

2 Purpose

2.1 This policy standardises how Dundalk Institute of Technology will manage SAR's so as to ensure that:

2.1.1 Data Subjects are provided with a clear, efficient and easy to use means of requesting access to their personal information.

2.1.2 SAR's received by the Institute are recognised, logged and acknowledged in a timely manner.

2.1.3 The location and retrieval of personal data within the scope of a SAR is efficient and thorough.

2.1.4 Staff asked to provide information in response to a SAR is aware of their duties and responsibilities to comply with the requests.

2.1.5 Responses to SARs are consistent and fully deliver against the rights of the individuals.

2.1.6 Any exemptions to the rights to access are applied appropriately and documented accordingly.

3 Definitions

3.1 The following definitions apply to this policy:

3.1.1 Personal Data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.1.2 General Data Protection Regulations (GDPR) is an EU regulation intended to strengthen the protection of personal data that applies to the processing carried out by organisations operating within the EU and to organisations outside the EU that offer goods or services to individuals in the EU.

4 Scope

4.1 This policy and associated procedures applies to:

4.1.1 All staff, contractors, consultants, student workers, temporary workers, shared services, and data processors that have access to Institute systems or data.

4.1.2 All Data Subjects about whom the Institute processes personal data.

4.1.3 Data held on all Institute information and systems, whether hosted on site or in the cloud, on portable storage media or devices or paper.

4.1.4 Processing of data at all Institute locations and subsidiaries.

5 Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

Governing Body	To review and approve the policy on a periodic basis
Leadership Team	<p>The Leadership Team is responsible for the internal controls of Dundalk Institute of Technology an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. The LT is responsible for:</p> <ul style="list-style-type: none">• Reviewing and approving this Policy and any updates to it as recommended by the Data Protection Officer.• Ensuring ongoing compliance with the GDPR in their respective areas of responsibility.• As part of the Institute's Annual Statement of Internal Control, signing a statement which provides assurance that their functional area is in compliance with the

	<p>GDPR.</p> <ul style="list-style-type: none"> Ensuring oversight of data protection issues either through their own work or a Data Protection Oversight Committee or other governance arrangement.
Data Protection Officer	<ul style="list-style-type: none"> To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR To advise on all aspects of data protection and privacy obligations. To monitor and review all aspects of compliance with data protection and privacy obligations. To act as a representative of data subjects in relation to the processing of their personal data. <p>To report directly on data protection risk and compliance to executive management.</p>
Staff/Students/External Parties	<ul style="list-style-type: none"> To adhere to policy statements in this document. To report suspected breaches of policy to their Head of Department and/or Data Protection Officer.

If you have any queries on the contents of this Policy, please contact the Leadership Team or Data Protection Officer.

5.1 Roles pertaining to GDPR – Subject Access Request Policy

5.1.1 The Data Protection Officer will be the individual with operational responsibility for processing Subject Access Request in line with the requirements of the GDPR.

5.1.2 All staff are responsible for ensuring that they recognise a Subject Access Request and to forward it, or direct the requestor on to the Data Protection Officer immediately.

5.1.3 All staff that are requested by the Data Protection Officer to conduct a search for information and to provide it in response to a SAR, must do so and in the manner requested, as soon as they are contacted.

6 Receiving Requests

6.1.1 A SAR can be made in a number of different ways, including via telephone or in person, but for it to be considered a valid request, it must be clear what the data subject is requesting, they must provide proof of their identity so as to verify their right to access the data.

6.1.2 The Institute will always encourage the requestor to submit the request in writing so as to provide a clear audit trail of the request and to ensure that both the requestor and the Institute have a clear record of what was requested. If the requestor advises that a written request is not possible, the Institute DPO will liaise with them to facilitate an alternative method of submission.

6.1.3 Written requests may be received via letter, email or submission of the 'Subject Access Request Form' made available via the Institute website.

6.1.4 Where a request is considered too vague to be processed, the requestor shall be contacted to provide clarity. The request may not be considered valid until it is clear precisely what information is being requested.

6.1.5 Requests made by third parties acting on behalf of a data subject will be accepted, but they must be accompanied with a copy of written authority from the Data Subject or written authority such as Power of Attorney (if applicable) and proof of the Data Subjects identity. Requestors who cannot provide this will be refused until such time that they can.

6.2 Acceptable proof of identity shall be any of:

6.2.1 A copy of Photographic ID such as passport, driving licence or Student ID (originals are not required, but can be copied if presented in person).

6.2.2 Birth Certificate

6.2.3 Two utility bills or bank statements (with redacted transactions) containing a full address of less than 3 months old.

6.3 Requests made by third parties who are not acting on behalf of a data subject will be accepted, but they must be accompanied a letter showing their written authority to make such requests, for example An Garda Siochana and law enforcement agencies must state the exemption to the right to access under Irish law that they believe entitles them to access information.

6.3.1 The Data Protection Officer shall consider the validity of any request of this nature.

6.3.2 The Institute will refuse any requests that it considers does not engage the exemption stated in the request.

6.3.3 All Institute staff must familiarise themselves with the 'GDPR Guide to Subject Access Requests' so as to be able to recognise a SAR and direct the request to the DPO.

6.3.4 All SARs shall be logged on the Institute request log and acknowledged by the Institute with the expected date of response.

7 Fees

7.1.1 There is normally no charge for receiving a copy of information requested through SAR, however a 'reasonable fee' may be applied when:

7.1.2 A request is deemed to be manifestly unfounded, excessive or repetitive.

7.1.3 A request asks for further copies of the same information.

7.1.4 Any "reasonable fee" will be calculated based on the administrative cost of providing the information.

7.1.5 The Institute will notify the requestor of any reasonable fee within a month of the receipt of the original request, along with an explanation as to why the fee is applied.

8 Timescales

8.1 The time period to respond to a SAR begins upon receipt of a valid request.

8.1.1 If a request is sent to an account responding with an automatic 'out of office message' that contains a valid alternative contact, the person submitting the request is responsible for re-sending the request to the alternate email address.

8.1.2 Failure to send the email to the alternate email address will mean that the request will not be considered to have been "received".

8.2 Responses to SARs will be provided without delay and at the latest within one month (20 work days) of their receipt.

8.3 The period to respond to a request may be extended by a further two months where the request is considered complex or numerous.

8.4 The Institute will notify the requestor of any extension to the time to respond within a month of the receipt of the original request, along with an explanation as to why the extension is required.

9 Locating Requested Information

9.1 Once a valid request has been received, the DPO will establish the nature and likely location of the information the requester has asked for.

9.2 The DPO will contact the relevant system, process, or account owners that have been identified as likely to hold this information.

9.3 The DPO will explain what information is required and alert the relevant people on the deadlines that need to be met - usually no later than 10 working days before the deadline for disclosure.

9.4 Staff must not assume that information/emails in their account will be found in the accounts of another member of staff. Staff asked to search for information must carry out the search in full.

9.5 Where the request asks for "all emails held" and does not provide the names of the account holders, the DPO may instruct specialist staff in IT Services to conduct a search of the mail system to identify accounts possibly holding the relevant emails.

9.5.1 Staff will then be contacted by the DPO and asked to either provide copies of emails or to provide consent for IT services to provide copies of the emails.

9.6 The DPO will provide guidance and support to staff conducting searches, but it is the responsibility of individual staff members to search for and collate the information where possible.

9.7 If there are likely to be any issues in conducting the search, staff must notify the DPO immediately so that any requirement to extend the time to respond, or apply a fee, can be considered and the requestor notified within the month of receipt of the request.

9.8 An initial screening of the data should be completed prior to forwarding to the DPO to remove references (redact) any information that may pertain to another individual.

10 Screening Information

10.1 Once all information believed to be within the scope of the request has been returned to the DPO, it will then again be screened and reviewed for :

10.1.1 The presence of any third party data that the data subject is not entitled to receive and may result in the removal or redaction of such information unless:

10.1.1.1 The third party has consented to disclosure; or

10.1.1.2 It is reasonable in all circumstances to comply with the request without seeking the third party individual's consent.

10.2 The presence of any data that may be considered exempt from disclosure under the GDPR Irish DP law that will be removed or redacted before the information is disclosed.

10.3 The DP will be responsible for applying any exemptions if they are necessary and after taking advice.

11 Providing Information

11.1 Following screening, the DPO will collate the formal response to the request including:

11.1.1 A copy of the data and an explanation of any exemptions that have been applied.

11.1.2 A copy of the relevant Privacy Notice or any required additional description of:

11.1.2.1 The personal data concerning them.

11.1.2.2 The reasons why their data is being processed.

11.1.2.3 Details of anyone who has received or will receive their personal data.

11.1.2.4 Details of the origin of their data if it was not collected from them directly.

11.2 The format of the disclosure will be made in line with the requestor's preference whenever possible.

11.3 Where the requestor has not specified a preferred format, the Institute will provide the information using an appropriately secure electronic transfer method such as the HEAnet Filesender system.

11.4 The communication will set out the requestor's subsequent rights to:

11.4.1 Request another search if they believe information is missing.

11.4.2 Request that inaccurate information be rectified or erased.

11.4.3 The existence of any right to object to or restrict processing

11.4.4 Their right to complain to the Data Protection Commissioner if they are unhappy with the disclosure.

12 Data Processors and Subject Access Requests

12.1 When procuring a service provider to undertake work on behalf of the Institute, appropriate protocols will be agreed to ensure that data processors are aware of their responsibility to assist with subject access requests and to provide information (where necessary) that they may hold relevant to a subject access request received by the Institute.

13 Monitoring of SAR responses

13.1 The Data Protection Officer shall regularly review the handling of and responses to SARs, to ensure ongoing compliance, identify issues and ensure the quality and consistency of responses.

14 Policy Review

14.1 This policy will be reviewed every three years or sooner as is required e.g. where there are changes in legislation, or recommended changes to improve best practice.

This policy forms part of a framework of Data Protection Policies, procedures and guidance documentation which should be read in tandem with this policy. Attached as Appendix A.

Appendix A.:

The below is a list of a suite of policies and procedures that may be used in conjunction with this policy.

- Data Protection Policy
- Data Protection Procedures
- Data Protection Incident Response & Breach Notification Policy
- Data Encryption & Data Anonymisation and Pseudonymisation Policy
- Remote Access Policy
- Physical Access Policy
- Logical Access Policy
- Social Media Management
- Third Party Outsourcing
- Compliance
- Data Governance Policy
- Information Security Policy
- Wireless Security Policy
- Systems Development Life Cycle Policy
- Acceptable Usage Policy
- Privileged User Policy
- Information Security Policy
- Password Standard Procedures
- Anti-Virus Scanning and Protection Standards
- End User Guidelines
- Moderator Guidelines
- Change Control Procedures
- Data Backup and Monitoring Procedures
- User Administration Procedures
- Incident Handling Procedures
- Access to IT Services

The above list is not exhaustive and other Dundalk Institute of Technology policies, procedures and standards and documents may also be relevant.