

Data Subject Rights Procedure

Author/Responsibility	Document Version	Date Reviewed	Next Review Due
Lois McKean, Data Protection & Information Compliance Officer	1.7	Feb 26	Feb 29
Approved at SWG: 19 January 2026			

1.0 BACKGROUND

- 1.1 North West Regional College must process many categories of personal data to provide education, training and employment. It regards the lawful and correct treatment of personal information as imperative to successful operations and to maintaining confidence between all data subjects and the College. We ensure that our organisation treats information it processes lawfully and correctly.
- 1.2 The UK General Data Protection Regulations ('UK GDPR') provides individuals with statutory Rights which can be exercised at any given time.
- 1.3 These Rights are:
 1. The Right to be Informed
 2. The Right of Access
 3. The Right to Rectification
 4. The Right to Erasure
 5. The Right to Restrict Processing
 6. The Right to Data Portability
 7. The Right to Object
 8. Rights in Relation to Automated Decision Making and Profiling
- 1.4 The College must acknowledge and respond to all requests within the provisions of the regulations.
- 1.5 There may be occasions when an exemption, legal requirement or overarching business need applies which, in turn, restricts the extent of the College meeting the data subject's wishes however all requests will be considered on a case by case basis.
- 1.6 All requests in relation to Data Subject Rights (DSR) must be processed and responded to without undue delay and in any event within one calendar month of receipt of the request. In exceptional circumstances, the timeframe may be extended by one additional month.
- 1.7 This Procedure provides guidance on the process to be followed when a Data Subject makes a request in relation to his/her rights as per UK GDPR.
- 1.8 The College must not destroy information as a result of an individual exercising their Rights. It is a criminal offence if destroyed after a request has been made.
- 1.9 Exemptions to the format of the request may apply under the Disability Discrimination Act 1995.

2.0 SCOPE

- 2.1 Data Subject Rights can be exercised by any individual whose personal data is being processed by North West Regional College.
- 2.2 This Data Subject Rights Procedure applies to all North West Regional College employees.
- 2.3 Once the request has been transferred to the Data Protection and Information Officer (DPO), the procedures scope is limited to the DPO and data custodians. The data custodian is usually the person responsible for, or the person with administrative control over, granting access to the College's documents or electronic files while protecting the data as defined by the College's security policy or its standard IT practices.

NWRC Data Protection & Information Compliance Officer contact details are:

Lois McKean
Data Protection & Information Compliance Officer (DPO)
North West Regional College
Strand Road
Derry~Londonderry
BT48 7AL

Email: dpo@nwrc.ac.uk
Tel: 02871 276154

3.0 PROCEDURE

3.1 Receipt of a Request

For the purposes of demonstrating accountability, transparency and good record keeping, the College would ask for all DSR requests to be submitted in written format. If an individual makes a verbal request the College will follow up in writing asking the individual to confirm our understanding and detail of what is being asked. Requests will not be actioned until confirmation from the requester has been received.

The requester does not have to quote reference to the UK GDPR or Data Protection legislation to have the request treated as such.

Staff should consider if this is a legitimate request or a routine business enquiry and contact the DPO for guidance where there is uncertainty.

Once determined as a legitimate DSR request, it should be forwarded to the DPO who will assume responsibility for overseeing the request and providing a response.

3.2 Check that the Request is Within the Scope of UK GDPR

Before proceeding with the request, the DPO will verify the following:

- a. It provides sufficient information to verify the data subject's identity; and
- b. It provides sufficient information to enable the College to locate, assess and action the relevant scope of the request.

3.3 Verify the Identity of the Data Subject

Before processing the request, the identity of the data subject must be verified. Whilst it is important that we do not communicate personal information to people who are not the data subject, we must not appear obstructive. The College should take reasonable measures to verify the data subject's identity and will keep a record of what measures we take.

The College can often verify an individual's identity from their circumstances, e.g. address, signature, student ID. If this is not possible, we can write to the individual asking them to send the College a photocopy of some form of identification such as their passport or driving licence.

It is important to note if the data subject is making the request or if the request being made on behalf of the person. If a third party is making the request, the College will only respond where there is a legal basis to do so. This will normally be 'consent' of the data subject.

There may be occasions where this measure is not required e.g. a staff member making a request via their College email account.

3.4 Clarify the Request

If the request is unclear or is very broad, the College may contact the applicant to seek clarification or a reformulation of their request. This can be done by telephoning the applicant or in writing. For the purposes of recording the rationale behind how we respond to a request, it would be preferable to do this in writing.

Where further information is required before a search can be undertaken or a clear understanding of the request is required, the data subject should be contacted within 5 working days of receipt. Please note: a 'working day' is any day other than a Saturday, Sunday (weekends) and public holidays. A 'working day' is considered to end at 23:59.

Where clarification is required the requester will be asked to respond within 5 working days from the date clarification is being sought. The month deadline for response will be re-calculated to begin from the date the clarification is received.

Seeking clarification will not be used as a means of allowing the College extra time to locate and review the information.

3.5 Calculate the Deadline for Response

A response must be issued without delay and within a maximum time of 1 month from the date the request or clarification is received.

The due date for the response should be calculated. The calculation for a 'month' will be calculated by counting one calendar month from the date of receipt (e.g. if the request is received on 4th March, the response will be due by 4th April).

3.6 Record DSR Request

The date the request is received must be recorded to evidence the timescale for response. The clock begins from the date of receipt by the College, not by the DPO. Therefore, it is imperative that confirmed or suspected DSR requests are forwarded to the DPO within 24 hours or as soon as possible.

The DPO will;

- a. Input the request details on to the designated recording system.
- b. Note the deadline for reply against the record.
- c. Acknowledge receipt of request (the acknowledgement letter should be completed no later than 5 working days from receipt of the request).
- d. All elements of each request will be recorded on the designated recording system to support the decision, actions taken and communications.

Staff on holidays during term time and during the summer period should ensure that their out of office is enabled on Outlook and that a forwarding contact is provided to ensure requests are dealt with as soon as possible.

3.7 Determine the Information

How each DSR request is handled will depend on the category within which it falls. When searching for personal information about the applicant, we may need to search central filing systems, personnel records and shared databases to locate the requested data. The DPO may also need to speak to members of staff across different departments who might hold information about the individual.

Upon assessing the scope of the request, the DPO may contact the IT Services Department to arrange for a 'litigation hold' to be activated on College systems to protect information within the scope of the request. The 'litigation hold' will be deactivated once the process of information extraction, response to the request and any appeal matters have been concluded.

Staff who hold requested information must declare everything which falls into the scope of the request. Information must not be deleted or access obstructed to hinder the College meeting its legal obligation towards individuals' rights afforded by UK GDPR.

The following is guidance, however the DPO (or delegates) may operate discretion, flexibility and extra measures as each request will vary.

1. The Right to be Informed¹

- i. This request may be an individual asking questions such as how we are processing their data, why are we carrying out a certain processing activity, querying our legal basis or who their data may be shared with etc.
- ii. The College has a Privacy Notice on the website which individuals can be directed to. It will contain the broad, high volume or significant processing activities of the College.
- iii. For activities not included on the Privacy Notice, the DPO will contact the relevant Head of Department or relevant manager to determine the background to the processing.
- iv. There may be exemptions of a data subjects right to be informed e.g. where the processing is subject to criminal investigation. Such considerations will be reliant on thorough co-operation of all relevant staff.

¹ [UK GDPR Articles 13 & 14 \(Information & Access to Personal Data\)](#)

2. The Right of Access²

- i. The DPO will identify the individual's relationship with the College e.g. staff, student, customer as this will help identify where personal information about the individual might be held and locate that information.
- ii. The DPO or nominee may need to search relevant filing systems, personnel records and shared databases.
- iii. The DPO or nominee may also need to speak to members of staff across different departments who might hold information about the individual.
- iv. It is imperative that the data custodians inform the DPO if there are risks associated with certain disclosures. The DPO can then determine if there is an existing exemption to protect the information.

3. The Right to Rectification³

- i. The data subject has a right to ask for inaccurate information to be corrected.
- ii. Once it is clear what information is being queried, the DPO should contact the lead custodian of that data.
- iii. Consideration should be given by all parties involved as to the scope of the request, i.e. does the information stretch beyond one department, are third party processors involved and if so, they should also be notified.
- iv. There may be occasions where the information cannot be changed however a note may be put against the data to reflect the inaccuracy.

4. The Right to Erasure⁴

- i. This Right may be more commonly recognised as the 'Right to be Forgotten' and may be referred to as such by the requester.
- ii. If the data subject has reason to believe their information is being processed without a legitimate basis, they may ask for the data to be deleted or removed.
- iii. In some circumstances the College may have an overarching business need to either partially delete the data or not at all. Such cases may include:
 - a. We have a legal obligation to retain the information
 - b. Public interest is better served by keeping it on record
 - c. Information is required to substantiate or refute a legal claim
- iv. Consideration should be given by all parties involved as to the scope of the request i.e. does the information stretch beyond one department, are third party processors involved and if so, they should also be notified.
- v. The DPO and data custodians must consider the impact of erasure and together record the rationale behind the final decision.
- vi. Regardless of the final decision, the DPO will either confirm deletion or communicate our rationale for our need to keep the information active.

² [UK GDPR Article 15 \(Right of Access\)](#)

³ [UK GDPR Article 16 \(Right of Rectification\)](#)

⁴ [UK GDPR Article 17 \(Right of Erasure\) / Right to be Forgotten](#)

5. The Right to Restrict Processing⁵

- i. This Right allows individuals to request a halt on the processing of any personal information which they consider to be inaccurate, unlawful or to defend or refute a legal claim and they do not wish for the data to be deleted.
- ii. This list is not exhaustive and all requests should be considered.
- iii. The DPO and data custodians must look at the areas where the information is processed e.g. departments, systems, files
- iv. The College will be permitted to retain the data but further processing will not take place.
- v. We will also keep a record of information to ensure this Right is respected in future processing by our organisation.

6. The Right to Data Portability⁶

- i. An individual who registers with another service provider may request that their information is transferred to them directly.
- ii. The right to data portability only applies:
 - a. to personal data an individual has provided to a controller;
 - b. where the processing is based on the individual's consent or for the performance of a contract; and
 - c. when processing is carried out by automated means.
- iii. The DPO should contact the data custodian, this will primarily be I.T to determine the process required to meet this request.
- iv. Information may be electronically transferred to the third party safely and to the point of being re-used by them.
- v. We will provide the personal data in a structured, commonly used and machine readable format. Machine readable means that the information is structured for software to extract specific categories of information. The new service provider should in turn, be able to re-use the information we have provided to them.
- vi. We may be able to transmit the data directly to another organisation if this is technically feasible. This will be considered on a case by case basis depending on the software available to both parties.

7. The Right to Object⁷

- i. If an individual believes our public task is unfounded or they wish to have their details removed from direct marketing campaigns or research/statistical processing, this Right gives them the opportunity to object to these processing activities.

⁵ [UK GDPR Article 18 \(Right to Restrict Processing\)](#)

⁶ [UK GDPR Article 20 \(Right to Data Portability\)](#)

⁷ [UK GDPR Article 21 \(Right to Object\)](#)

- ii. *Processing for performance of a legal task or Public Authority purpose.*
 - a. We will grant the request unless there is a legitimate basis for the College to continue the processing or if the processing is required to settle a legal claim.
 - b. This legal purpose can be confirmed with the data custodian
- iii. *Rights in Relation to Direct Marketing*
 - a. If an individual wishes for their details to be removed from our marketing lists, we will comply with your request immediately and no further advertising/marketing should be issued by the College to that individual.
 - b. These requests must be communicated to the relevant Departments (including Marketing) immediately and mailing lists updated with this new preference.
 - c. The list of subscribers and mailing preference lists should be refreshed immediately prior to future advertising/ marketing communications.
- iv. *Rights in relation to statistical/research purposes*
 - a. If the College has reason to process personal information for this reason, we will consider all requests and where possible grant a request unless it is necessary for the performance of a public task.

8. Rights in Relation to Automated Decision Making and Profiling⁸

- i. If personal information is subject to automated decision making, i.e. there is no human involvement, individuals have a right to ask for a person to review the information and make a fresh decision.
- ii. The College cannot guarantee a different outcome but human intervention may explain rationale to the individual.
- iii. There are some instances where this Right does not apply, such as:
 - a. The processing is necessary for contractual purposes
 - b. The processing is based on consent

Further guidance on all such Rights is available on the ICO website⁹

3.8 Review information considering possible exemptions

- a. Once the College has identified the location of all information, we must consult with the data custodian and other relevant managers to discuss the impact of the request, e.g. if we can erase the requested data, if there is a legal basis for processing which prevents erasure and any the impact of disclosure.
- b. If the request relates to disclosure and the College considers this a risk, we must consider any relevant exemptions under legislation.

⁸ [UK GDPR Article 22 \(Automated individual decision-making, including profiling\)](#)

⁹ [A guide to individual rights | ICO](#)

- c. Exemptions must be considered on a case-by-case basis for each individual piece of information. In some cases, the College may be able to action elements of a request, but not all.
- d. If the College is asked to disclose information, only that which is about the person making the request should be released. We will redact personal data of any third party if a legal basis to process does not exist. Redaction should result in third parties being unidentifiable. Guidance on anonymisation is available in the FE Sector UK GDPR Handbook and the Information Commissioners Office (ICO) website¹⁰.

3.9 Responding to the Applicant

The applicant should receive a response in writing without delay and within a maximum time of 1 month from the date the request or clarification is received.

In relation to all other Rights' requests, individuals should be provided with either a confirmation that their request has been actioned or an explanation as to why the College is unable to process their request.

4.0 APPEALS PROCESS

- 4.1** If a requester is not happy with how the College has handled their request or exemptions applied to the response, they have a right to complain and to ask for an internal review of their request. Appeals should be submitted within 10 working days of receipt of response and detail reasons for dissatisfaction. This should be addressed to:

Lois McKean
Data Protection & Information Compliance Officer
North West Regional College
Strand Road Derry~Londonderry
BT48 7AL
Email: dpo@nwrc.ac.uk

- 4.2** The DPO will issue an Appeal acknowledgement within 5 working days from receipt of appeal.
- 4.3** The College will convene a panel of independent personnel (at least 2 members of staff) who will then examine the initial request/response, the request for appeal and review if there are areas for improvement and whether or not the College should reconsider its original response rationale.
- 4.4** The College will issue a response to all appeals within 20 working days from date of the acknowledgement letter being issued.
- 4.5** A 'working day' is any day other than a Saturday, Sunday (weekends) and public holidays. A 'working day' is considered to end at 23:59.

¹⁰ [Anonymisation | ICO](#)

- 4.6** If the requester is not happy with the Appeal Panel decision, they may contact the Information Commissioners Office (ICO) with a 'request for assessment' at:

The Information Commissioner's Office – Northern Ireland
3rd Floor
14 Cromac Place
Belfast
BT7 2JB

5.0 RECORDING ALL REQUESTS

Each request should be fully documented with the following:

1. Name/contact details of the requester
2. Nature of the request
3. Date request received/responded to
4. Copies of all correspondence between the College, the data subject and any other parties;
5. A record of any telephone conversations used to verify the identity of the individual or the information required, requests for additional information should be made in writing subsequent to telephone call;
6. A record of the College decisions and how we came to make those decisions e.g. application of exemptions;
7. If redactions have been made, copies of unredacted info should be retained;
8. Copies of information sent to the data subject.

6.0 COMMUNICATION PLAN

- 6.1 This procedure is available for staff on the College Intranet.
- 6.2 All staff to receive awareness raising and training to demonstrate an understanding of the requirements and responsibilities of the Data Protection and Freedom of Information legislation.

7.0 REVIEW

- 7.1 This Procedure will be reviewed every 3 years or sooner if required to reflect changes in legislation, circumstance or procedure.
- 7.2 The College will monitor all requests and comments for the purposes of quality control.
- 7.3 The DPO will conduct a regular evaluation of the process and activity to encourage continuous improvement.
- 7.4 The College will implement any remedial action as necessary in line with the outcome of the evaluation process.

In addition to being available on the Staff intranet, the above procedures will be communicated during staff induction and training.

Record of Changes				
Review Date	Page No.	Change Comment	Date of Change	Initials
06.01.26	Throughout	Minor edits / grammar / format changes	06.01.26	LMcK
06.01.26	Throughout	Update of job title for College DPO	06.01.26	LMcK
06.01.26	Throughout	Active online links to relevant legislation & ICO websites	06.01.26	LMcK
06.01.26	p.3 & p.8	Clarification on term 'working day'	06.01.26	LMcK
06.01.26	p.4	Clarification on liaison with IT Services to secure personal data for request	06.01.26	LMcK
06.01.26	p.4	Details of record of request retained	06.01.26	LMcK