NWSLC

NORTH WARWICKSHIRE & SOUTH LEICESTERSHIRE COLLEGE

Rights of Individuals Under the GDPR Policy 2025/26(v3)

North Warwickshire and South Leicestershire College

Policy Author: Data Protection Officer

Target Audience: Staff / Student / Public

Policy Location: Website /Staff SharePoint

Contents

Page

Rights of Individuals under the GDPR Policy 2025/26(v3)

1. Introduction 1
2. Scope 1
3. Definitions 1
4. Related Policies, Procedures and Documents 1
5. Rationale 2
6. Staff Responsibilities 2
7. Individuals' Rights Over Their Personal Data 2
   - 7.1 Right of Access (Subject Access Requests - SAR) 2
   - 7.2 The Right Relating to Decision Making 4
   - 7.3 The Rights Relating to Automated Decision Making 4
   - 7.4 The Right to Object - Processing Of Personal Data 5
   - 7.5 The Right to Object - Direct Marketing 5
   - 7.6 Processing Based Upon Public Task Or Legitimate Interests 6
   - 7.7 Right to Rectification 6
   - 7.8 Right to Erasure (Right to be Forgotten) 6
   - 7.9 Right to Restrict Processing 7
   - 7.10 Right to Data Portability 8
8. Equality Analysis 9
9. Implementation, Monitoring and Review 9

Document History

Version Number	Amended By	Date of Revision	General Revision Description
V2	Clerk to the Corporation	8.1.22	Minor formatting changes
v3	Clerk to the Corporation	25.11.25	Minor updating changes to dates Changes in text, in line with current ICO guidance Change from three yearly to annual review.

Rights of Individuals under the GDPR Policy 2025/26(v3)

1. Introduction

1.1 North Warwickshire and South Leicestershire College's (the College) reputation and future growth are dependent on the way the College manages and protects personal data.

1.2 All individuals have rights over their personal data and the College recognises the importance in having an effective Policy in place to allow individuals to exercise these rights in a way that is clear and easy for them.

1.3 The College has therefore implemented this Policy to ensure all College staff are aware of:

i. the rights individuals have over their personal data and;

ii. how the College will ensure that those rights can be exercised.

1.4 College staff will receive a copy of this Policy when they begin to work at the College and may receive periodic revisions of this Policy.

1.5 This Policy does not form part of any member of staff's contract of employment and the College reserves the right to amend this Policy at any time.

1.6 All College staff are obliged to comply with this Policy at all times.

2. Rationale

2.1 The College's General Data Protection Regulation Policy is the College's fundamental policy, which sets out:

i. the types of personal data that the College may be required to handle;

ii. the College's legal purposes for doing so;

iii. how the College complies with its obligations under the Data Protection Laws.

2.2 This Policy explains how the College complies with its legal obligations to allow individuals to exercise their rights over their personal data.

2.3 The College has a corresponding Rights of Individuals under the GDPR Procedure. This sets out the processes the College follows to respond to individuals exercising the rights set out in this Policy.

3. Scope

3.1 This Policy applies to all College staff who collect and / or use individuals personal data, which is stored electronically, in paper form or otherwise.

4. Definitions

4.1 College staff - any College employee or contractor who has been authorised to access any personal data and will include employees, consultants, contractors and temporary staff hired to work on behalf of the College.

4.2 Data Protection Laws - the General Data Protection Regulation and all applicable laws relating to the collection and use of personal data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

4.3 Data Protection Officer (DPO) - the DPO can be contacted at 02476 243000 or by email at dpo@nwslc.ac.uk.

4.4 ICO - the Information Commissioner's Office, the UK's data protection regulator.

4.5 Personal data - any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious belief. It also includes information that allows an individual to be identified indirectly, for example an identification number, location data or on online identifier.

4.6 Processing - any collection, use or storage of personal data, whether on the College's information systems or in paper form.

4.7 Special categories of personal data - personal data which reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images or fingerprints), physical or mental health, sexual life or sexual orientation and criminal record.

5. Related Policies, Procedures and Documents

5.1 GDPR Policy;

5.2 Rights of Individuals under the GDPR Procedure;

5.3 Freedom of Information Policy;

5.4 Retention of Information Schedule;

5.5 IT Security Policy.

5.6 Other policies and documents may be identified from time to time as circumstances change and may be added to this list.

6. Staff Responsibilities

6.1 This Policy sets out the rights that individuals have over their personal data under Data Protection laws. If a member of staff receives a request from an individual to exercise any of the rights set out in this Policy, that member of staff must:

i. notify the Data Protection Officer as soon as possible and, in any event, within 24 hours of receiving the request;

ii. inform the Data Protection Officer as to what the request consists of, who has sent the request and provide the DPO with a copy of the request;

iii. not make any attempt to deal with or respond to the request without authorisation from the Data Protection Officer.

7. Individuals' Rights Over Their Personal Data

7.1 **Right of Access (Subject Access Requests - SAR)**

7.1.1 7.1.2 The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. Under this right, individuals can obtain the following:

i. confirmation that the College is processing their personal data;

ii. a copy of their personal data in intelligible form, (this includes providing an explanation of any technical terms or jargon which might otherwise obscure its meaning to the reader); and

iii. other supplementary information (this largely corresponds to the information the College provides in a privacy notice);

iv. the legal basis on which the College is processing their personal data;

v. the purposes for which the College is holding their personal data;

vi. the categories of personal data that the College is holding about them;

vii. the recipients or categories of recipients that their personal data has been or will be disclosed to;

viii. the retention period for storing the personal data or, where this is not possible, the criteria for determining how long the College will store it;

ix. that they have the right to request the College to correct any inaccuracies in the personal data (see 7.2) or deletes their personal data (see 7.3); or restrict the uses the College is making of the personal data (for the circumstances when this can happen see below for further information); or to object to the uses the College is making of their personal data (for the circumstances when this can happen see below for further information);

x. that they have the right to complain to the ICO if they are unhappy about the way the College has dealt with this request or in general about the way the College is handling their personal data;

xi. where the personal data was not collected from the data subject, where the College obtained it from; and

xii. the existence of automated decision-making including profiling (if applicable);

xiii. the safeguards the College has provided where personal data has or will be transferred to a third country or international organisation.

xiv. The College will comply with a subject access request (SAR) by providing the individual with a copy of their data in writing, unless:

- this is not possible;
- would involve disproportionate effort; or
- the individual agrees to receive it in another form.

xv. The College can charge a fee for a SAR. The level of this fee may be set by the Secretary of State in regulations but, in the absence of any such regulations at this time, the maximum fee is set at £10.

xvi. The College may ask for information to verify an individual's identity. The request for information will be reasonable and proportionate regarding what is asked for.

xvii. The timescale for responding to a SAR does not begin until the College has received the requested information. A request ID documents when required, will be made promptly.

xviii. The College may also ask for additional information in order to identify and locate the data that is being requested; particularly where the request is phrased in very broad and general terms. The timescale for responding to a SAR doesn't begin until the College has received the additional information. Any request for additional information will be made promptly.

xix. Where the College has previously complied with a request, it will not respond to a repeat request for the same information, unless a reasonable interval has elapsed. When deciding whether a reasonable interval has elapsed the following matters will be considered:

- the nature of the data (including whether it is particularly sensitive);
- the purpose for which the data is being processed; and
- how often the data is altered.

xx. Where it is unlikely that the data has changed between requests, the College may decide it does not need to respond to the same request twice. Where data has been deleted since the last request, the College will inform the individual of this.

xxi. The College will provide the information to the individual 'promptly' and, in any event, within one calendar month of receiving it (i.e. within one calendar month of the day the College received the request). If the College has requested a fee, additional

identification, or further information to locate the data requested, the one month time period begins on the day you receive it.

xxii. If the College is unable to comply with a request, the individual will be informed about:

- the reasons why (where possible);
- their right to make a complaint to the ICO; and
- their ability to seek to enforce this right through the courts.

xxiii. Where the College is relying on an exemption to refuse to comply with a SAR, where possible the College will explain the reasons why it considers this exemption applies. This will however depend on the specific circumstances of the request. In some situations, the College's response may be more general and may not include details of which exemptions have relied on at all. For example, where telling an individual that it has applied a particular exemption which would prejudice the purpose of that exemption.

7.2 **The Right Relating to Decision Making**

7.2.1 Where the College is processing data and applying the results to an individual, they have the right to know the reasoning underlying that processing. This applies whether the processing and results (or decision-making) are automated or not. There isn't a requirement to proactively give this information to the individual, but if it is requested the College will provide it promptly and without undue delay.

7.3 **The Rights Relating to Automated Decision Making**

7.3.1 The College will not make any decision solely by automated means that significantly affects an individual, unless:

i. the decision is required or authorised by law;

ii. the individual has given consent to the decision being made this way; or

iii. it is needed for entering into or performing a contract with the individual.

7.3.2 Automated decision making is where decisions are made about individuals automatically, and without human input or intervention. This is distinct from "automated processing" (e.g. the collection, storage, or other processing by IT systems or other automated means), although automated processing will be involved in automated decision-making.

7.7.3 Profiling happens where the College automatically used personal data to evaluate certain things about an individual.

7.3.4 If the automated decision is required or authorised by law, the College will notify individuals that such a decision has been made and that they have a right to request human intervention in that decision-making. They can request the decision is reconsidered, or request that a new decision is taken which isn't based solely on automated processing.

7.3.5 The College must consider any request, including any relevant additional information the individual provides, and inform them in writing of the outcome of that consideration.

7.3.6 This right to be notified, and to have intervention, doesn't apply if the automated decision-making was done:

i. with the consent of the individual; or

ii. for the purposes associated with entering into or performing a contract with them.

7.3.7 Before the end of one month from the date the College gets the request, the College must notify the individual in writing that the College has complied or intends to comply with their objections or that the College is not complying and the reason why.

7.4 **The Right to Object - Processing Of Personal Data**

7.4.1 Individuals have the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent the College from processing their personal data.

7.4.2 The right to object only applies in certain circumstances. Whether it applies depends on the College's purposes for processing and its lawful basis for processing.

7.4.3 Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

7.4.4 Individuals can also object if the processing is for:

i. a task carried out in the public interest;
ii. the exercise of official authority vested in you; or
iii. your legitimate interests (or those of a third party);

however in these circumstances the right to object is not absolute.

7.4.5 Individuals have the right to object to the processing of their personal data (either in general or in relation to a specific purpose), on the grounds that they believe that the processing is an unwarranted interference with their rights or interests.

7.4.6 An individual must inform the College of their specific reasons why they believe the processing constitutes an interference, and why it is unwarranted in the circumstances.

7.4.7 If the College receives an objection it will consider it and it may continue with the processing while the objection is being considered.

7.4.8 If the College agrees to the objection, it will stop the processing. If, having carefully considered the necessity and proportionality of the processing, the College decides that in the circumstances the processing is not an unwarranted interference, it will continue processing.

7.4.9 Whether or not the College agrees with the objection, it will inform the individual of its decision within 21 days, and give its reasons.

7.4.10 If the College needs to verify the ID of the requester, or needs further information to locate the data in question, this period will not start until the College has received the information it reasonably requires.

7.5 **The Right to Object - Direct Marketing**

7.5.1 An individual can object to the processing of their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

7.5.2 This is an absolute right and there are no exemptions or grounds for the College to refuse. Therefore, when it receive an objection to processing for direct marketing, it will not process the individual's data for this purpose.

7.5.3 This however does not automatically mean that the College needs to erase the individual's personal data, and will in most cases suppress that individual's details. Suppression involves retaining just enough information about the individual to ensure that their preference not to receive direct marketing is respected in future.

7.6 **Processing Based Upon Public Task Or Legitimate Interests**

7.6.1 An individual can also object where you are relying on one of the following lawful bases:

i. 'public task' (for the performance of a task carried out in the public interest),

ii. 'public task' (for the exercise of official authority vested in you), or

iii. legitimate interests.

7.6.2 An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation. In these circumstances this is not an absolute right, and you can refuse to comply if:

i. you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or

ii. the processing is for the establishment, exercise or defence of legal claims.

7.6.3 If you are deciding whether you have compelling legitimate grounds which override the interests of an individual, you should consider the reasons why they have objected to the processing of their data. In particular, if an individual objects on the grounds that the processing is causing them substantial damage or distress (eg the processing is causing them financial loss), the grounds for their objection will have more weight. In making a decision on this, you need to balance the individual's interests, rights and freedoms with your own legitimate grounds. During this process you should remember that the responsibility is for you to be able to demonstrate that your legitimate grounds override those of the individual.

7.6.4 If you are satisfied that you do not need to comply with the request you should let the individual know. You should explain your decision, and inform them of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

7.7 **Right to Rectification**

7.7.1 Individuals have the right to request the rectification of their personal data if they believe it is inaccurate

7.7.2 Where the individual tells the College that their personal data is incomplete, the College is obliged to complete that data if the individual asks the College to do so. This may mean adding a supplementary statement to their personal file for example.

7.7.3 If the College has disclosed the individual's inaccurate personal data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties of the correction, where the College can.

7.7.4 Where an individual asks the College to correct their personal data, the College is required to do so and to confirm this in writing to the individual within one month of them making the request.

7.8 **Right to Erasure (Right to Be Forgotten)**

7.8.1 Individuals have the right to request the erasure of their personal data if they believe the processing of the data contravenes any of the data protection principles. The right to be forgotten applies when:

i. the personal data is no longer necessary for the purpose the College has collected it for;

ii. the individual withdraws consent and the College has no other legal basis to use their personal data;

iii. the individual objects to the College's processing and there is no overriding legitimate interest for continuing the processing;

iv. the personal data was unlawfully processed;

v. you have objected to the use of your data for direct marketing purposes;.

vi. the personal data has to be erased to comply with a legal obligation.

vii. The data was collected from you as a child for an online service.

7.8.2 If the College has disclosed the individual's deleted personal data to any third parties, the College is required to tell the individual who those third parties are and to inform the third parties to delete the personal data, where the College can.

7.8.3 When an individual asks the College to delete their personal data, the College is required to do so and to inform the individual in writing within one month of them making the request this this has been done.

7. 9 **Right to Restrict Processing**

7. 9.1 Individuals have the right to 'block' or 'suppress' the College's processing of their personal data when:

i. they contest the accuracy of the personal data, for a period enabling the College to verify the accuracy of the personal data;

ii. the processing is unlawful and the individual opposes the deletion of the personal data and requests restriction instead;

iii. the College no longer needs the personal data for the purposes the College collected it for, but the College is required by the individual to keep the personal data for the establishment, exercise or defence of legal claims;

iv. the individual has objected to the College's legitimate interests, for a period enabling the College to verify whether its legitimate interests override their interest.

7.9.2 If the College has disclosed the individual's restricted personal data to any third parties, the College is required to tell the individual who those third parties are, and to inform the third parties about the restriction, where the College can.

7.9.3 When an individual asks the College to restrict its processing of their personal data, the College is required to do so and to confirm to the individual in writing within one month of them making the request that this has been done.

7.9.4 A request may be manifestly unfounded if:

i. the individual clearly has no intention to exercise their right to restriction. For example an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or

ii. the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example:

iii. the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;

iv. the request makes unsubstantiated accusations against you or specific employees;

v. the individual is targeting a particular employee against whom they have some personal grudge; or

vi. the individual systematically sends different requests to you as part of a campaign, eg once a week, with the intention of causing disruption.

vii. the word "manifestly" means there must be an obvious or clear quality to it being unfounded. You should consider the specific situation and whether the individual genuinely wants to exercise their rights. If this is the case, it is unlikely that the request will be manifestly unfounded.

7.9.5 A request may be excessive if:

i. it repeats the substance of previous requests; or

ii. it overlaps with other requests.

iii. However, it depends on the particular circumstances. It will not necessarily be excessive just because the individual:

iv. makes a request about the same issue. An individual may have legitimate reasons for making requests that repeat the content of previous requests. For example, if the controller has not handled previous requests properly;

v. makes an overlapping request, if it relates to a completely separate set of information; or

vi. previously submitted requests which have been manifestly unfounded or excessive.

vii. What should we do if we refuse to comply with a request for restriction?

viii. You must inform the individual without undue delay and within one month of receipt of the request.

ix. You should inform the individual about:

- the reasons you are not taking action;

- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

You should also provide this information if you request a reasonable fee or need additional information to identify the individual. 7.10 **Right to Data Portability**

7.10.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. Individuals have the right to obtain from the College, a copy of their own personal data in a structured, commonly-used and machine-readable format (such as CSV files[1]). The aim of this right is to facilitate the ability of individuals to move, copy or transmit their personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

7.10.2 The right to data portability only applies when

i. the individual provided the College with the personal data or is personal data resulting from observation of an individual's activities (e.g. where using a device or service) but does not include It does not include any additional data that you have created based on the data an individual has provided to you;

ii. the processing the College is carrying out is based on the individual's consent or is necessary for the performance of a contract; and

iii. the processing is carried out by automated means (i.e. excluding papers files).

7.10.3 This means that the right to data portability does not apply to personal data the College is processing on another legal basis, such as legitimate interests and information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to you..

7.10.4 The College is obliged to provide this information free of charge within one month of the individual making the request (or two months where the request is complex, provided the College explains to the individual why it needs more time).

7.10.5 The individual also has the right to ask the College to transmit the personal data directly to another organisation if this is technically possible.

8. Equality Analysis

8.1 By virtue of the provisions of the Equality Act 2010, the College has a duty to have due regard to the need to:

i. eliminate unlawful discrimination, harassment and victimisation and other prohibited conduct;

ii. advance equality of opportunity between people of different groups;

iii. foster good relations between people from different groups.

8.2 In implementing this Policy and associated procedures, the College will actively take these aims into account as part of its decision making process and will demonstrate how this has been undertaken.

8.3 Where necessary a full equality impact assessment will be undertaken.

9. Implementation, Monitoring and Review

9.1 Activity taking place under this Policy will be reviewed by the DPO and reported to the Executive on a termly basis and the Corporation on an annual basis.

9.2 This Policy will be reviewed every three years, or as otherwise directed by the Principal, College policy or regulatory or legislative changes.

[1] CSV files are comma-separated values files - CSV is a simple file format used to store tabular data, such as a spreadsheet or database. Files in the CSV format can be imported to and exported from programs that store data in tables, such as Microsoft Excel.