NWSLC

NORTH WARWICKSHIRE & SOUTH LEICESTERSHIRE COLLEGE

Data Protection Complaints Procedure 2026/27(v1)

North Warwickshire and South Leicestershire College

Title of Policy Author and Lead Owner: Data Protection Officer

Target Audience: Staff / Students / Public

Policy Location: Website / Staff SharePoint

Implementation Date: March 2026

Contents

Data Protection Complaints Procedure 2026(v1)

Page

1. Introduction 1
2. Rationale and Aims 1
3. Definitions 1
4. Core Principles 1
5. Data Protection Complaints Procedure - How To Complain 2
6. Proof of Identity Requirement 2
7. Complaints From or On Behalf of Children 3
8. Responsibilities 3
9. Investigation and Complaint Outcomes 3
10. Review 4
11. Independent External Review 4
12. Manifestly Unfounded, Abusive, Vexatious or Excessive Correspondence 4
13. Use of Data from Complaints 5
14. Monitoring and Reporting 5
15. Implementation and Review 5
16. Right To An External Review 5

Document History

Version Number	Amended By	Date of Revision	General Revision Description
1.	-	March 2026	Implementation of the Procedure

Data Protection Complaints Procedure 2026/27

1. Introduction

1.1 As from 19th June 2026, where organisations hold personal data the Data Use and Access Act 2026 now requires those organisations to:

i. provide complainants with a procedure by which to make data protection complaints;

ii. acknowledge receipt of complaints within 5 days of receiving them; and

iii. without undue delay:

- take appropriate steps to respond to complaints, including making appropriate enquiries and keeping complainants informed; and
- inform complainants of the outcome of their complaints.

1.2 This procedure sets out how complainants can raise complaints about the handling of their personal data in line with the requirements of the Data Use and Access Act 2026.

2. Rationale and Aims

2.1 North Warwickshire and South Leicestershire College (the College) recognises the importance of implementing a clear complaints processing procedure, enabling data subjects to raise complaints about the handling of their personal data.

2.2 Having a procedure for dealing with data protection complaints enable the College to be accountable and improve dialogue with those who wish to make a complaint. It will also enable the building of trust around how the College handles individuals' personal data and lead to fewer complaints to the Information Commissioner's Office (ICO).

2.3 The College is committed to handling personal data in accordance with data protection law. The aims of this procedure are to:

i. provide guidance to College staff when dealing with a data protection complaint;

ii. ensure staff engage with such complaints positively and proactively; and

iii. enable complainants to understand how to make a data protection complaint and the procedure which will be taken when they make a data protection complaint.

3. Definitions

3.1 **Data Protection Complaint**: a complaint from a data subject (or an authorised third party) expressing dissatisfaction about the College's handling of their personal data or the data of the individual they represent. This can also include dissatisfaction with how the College has responded to a previous data request.

3.2 **Data Subject**: any living individual whom the personal data held by the College, is about.

3.3 **Personal Data**: information about an identified or identifiable living individual held on computer or in a structured filing system, examples would include: names, contact information including emails and usernames, photographs, vehicle registration plates.

3.4 **Processing**: anything that can be done with personal data e.g. collecting, viewing, recording, organising, structuring, storing, altering, retrieving, sending, restricting or destroying it.

4. Core Principles

4.1 The College has put in place a procedure which enables complainants to make data protection complaints. This will include:

i. acknowledging receipt of complaints within 5 working days of receiving them; and

ii. without undue delay:

- taking appropriate steps to respond to complaints, including making appropriate enquiries and keeping complainants informed; and
- informing complainants about the outcome of their complaints.

5. Data Protection Complaints Procedure - How To Complain

5.1 Submission Process: the College has provided a clear, accessible method for individuals to submit complaints via the College website through the DPO mailbox, and to the DPO directly as the designated staff member.

5.2 Date of Submission: complaints should be submitted within two months of the issue arising, although in exceptional circumstances the DPO will consider complaints received outside this timescale.

5.3 Acknowledgment & Investigation: procedures are in place to acknowledge receipt of the complaint and investigate the matter.

5.4 Internal Review: this will involve a senior member of staff reviewing the DPO's findings and ensuring compliance before is final response is issued by the DPO.

5.5 Response Timelines: a formal response will be provided to the complainant within a specified, reasonable timeframe, generally within 30 days.

5.6 Escalation Path: complainants will be informed of their right to escalate the issue to the Information Commissioner's Office (ICO) if they remain dissatisfied. The new regulations encourage resolving issues directly with the College first.

5.7 Record Keeping: detailed records of all complaints, investigations, and outcomes will be kept to demonstrate compliance to regulators.

5.8 To make a complaint you should contact the College's Data Protection Officer in the following ways:

i. by email at dpo@nwslc.ac.uk; and

ii. via the College website on the 'Contact Us Page' https://www.nwslc.ac.uk/contact/

5.9 Data subjects and third parties may make a complaint relating to the College's use of personal data. Complaints should be sent directly to the Data Protection Officer. The DPO will normally acknowledge the complaint within 5 working days. The College reserves the right to extend the period for response during holidays and College closure.

5.10 Although a complaint may be brought at any time, there may be limits as to what the College can do in historic cases.

6. Proof of Identity Requirement

6.1 Where a complaint is from a data subject received a request for proof of identity will be made at the earliest opportunity. Examples of relevant proof of identify are passports, driving licences, College identity badges. These should be photographed or scanned and provided to the Data Protection Officer by email.

6.2 Where a third party (e.g. a family member or solicitor) makes a complaint on behalf of the complainant, the Data Protection Officer will check that they are authorised to act on the complainant's behalf. The required form of evidence will depend on the circumstances of each request, but some examples are a power of attorney or signed letter of authority from the data subject they are acting on behalf of. A request for proof of the identity of the data subject will also be required as set out in 6.1. above.

6.3 In line with ICO guidance, if there is no evidence that a third party is authorised to act on a complainant's behalf, the College is not required to investigate the complaint. In such circumstances, the DPO will respond to the request, explaining this point.

6.4 This procedure also addresses complaints made by third parties in relation to the College's use of personal data. These may be for example in relation to the College's response to a data related request from a third party, such as the Police or Local Government Agencies.

7. Complaints From or On Behalf of Children

7.1 If complaints are received from children, or on their behalf, we will ensure that we address children in plain, clear language that they can understand, throughout all stages of the process.

7.2 Although children have the same rights as adults over their personal information, they may be less aware of the risks, consequences and safeguards. We will therefore assess the capacity of the child to understand and exercise their rights in line with ICO guidance.(When may a child exercise their rights? in our children and the UK GDPR guidance).

7.3 If we receive complaints on behalf of a child, for example from a parent, another adult, or a representative such as a child advocacy service, charity or solicitor. We will consider the complaint in line with ICO guidance (When may a parent exercise these rights on behalf of a child.)

8. Responsibilities

8.1. The Chief Operating Officer has overall responsibility for this procedure but has delegated day-to-day responsibility for overseeing its implementation to the Data Protection Officer. All relevant members of staff have been made aware of the procedure and have received appropriate training.

8.2. All staff are responsible for:

i. Ensuring that any complaints made in relation to this procedure are reported to the Data Protection Officer and for co-operating with the Data Protection Officer in reviewing those complaints.

ii. Identifying and dealing with data protection complaints in accordance with this procedure, whether as first point of contact or person subsequently investigating and responding to the complaint.

8.3 The Data Protection Officer (DPO): is responsible for:

i. Triaging all data protection complaints to review their content and identify an appropriate case handler.

ii. Investigating and responding to all data protection complaints and liaising with the ICO regarding any data protection complaint referred to them.

iii. Logging all data protection complaints which are received.

9. Investigation and Complaint Outcome

9.1. Once all identification requirements have been met, an investigation of the matters raised in a complaint will normally be carried out within 30 working days of receiving relevant confirmation of identification.

9.2 If further clarification is required from the complainant or more time is required for the response to be completed the DPO will inform the complainant prior to the original deadline.

9.3 The DPO will endeavour to respond to a complaint as soon as possible and, in most cases, within one calendar month. If the complaint is particularly complex and further time is required to respond, then the DPO will keep the complainant informed.

9.4 The complaint outcome will be communicated to the complainant in writing and normally by email. The DPO will respond in writing providing details of the investigation undertaken and detailing the outcome of that investigation.

10. Review

10.1. If the complainant does not agree with the outcome, they can request a review of the decision. This request must be made within 1 month of the original decision being communicated and should be sent to the DPO. The decision will be internally reviewed by the Chief Operating Officer normally within 20 working days from the receipt of the request for review.

10.2. Once an internal review has been completed by the Chief Operating Officer, the outcome of that review will be communicated to the complainant in writing and normally by email.

11. Independent External Review

11.1. If the complainant remains dissatisfied, they can escalate their complaint to the Information Commissioner's Office (the "ICO"). Make a complaint | ICO

12. Manifestly Unfounded, Abusive, Vexatious or Excessive Correspondence

12.1. In some case the DPO can refuse to respond to a complaint. This will be when a complaint is deemed to be manifestly unfounded, abusive, vexatious or excessive. Each complaint will be considered on a case by case basis. The following factors will be taken into consideration:

i. the complainant has explicitly stated that they intend to cause disruption (whether in the complaint, or in other correspondence), and has threatened individuals;

ii. the complainant has made unsubstantiated accusations against individuals, and is persisting in those accusations;

iii. the complainant is targeting particular individuals, against whom they have a personal grudge;

iv. the complainant makes frequent complaints intended to cause disruption; and

v. the complainant continues to repeat the substance of previous complaints which have already been investigated.

12.2. Where a complaint is deemed to be manifestly unfounded, excessive, abusive or vexatious the DPO will contact the individual and in a reasonable timeframe explain to them:

i. the reason(s) for refusing to consider the complaint;

ii. their right to make a complaint to the ICO.

13. Use of Data from Complaints

13.1. The College will collect data on complaint outcomes at each stage of this procedure and any complaints submitted by complainants to any regulators (including the ICO), and use the data:

i. internally for reporting, evaluation, learning and training; and

ii. externally for discussion with regulators

13.2. The data used for the purposes set out above will be anonymised.

13.3 Personal data may be disclosed to the members of staff and regulators for the purpose of dealing with a complaint and implementing any recommendations.

13.4 Personal data will not be shared with any other third parties unless the College has:

i. received express consent from the data subject to do so;

ii. a statutory obligation to do so,

iii. is otherwise permitted to do so under the Data Protection Act.

14. Monitoring and Reporting

14.1 All data protection complaints shall be reviewed by the DPO in accordance with this procedure and their advice shall be followed accordingly.

14.2 The DPO shall review all other complaints on a termly basis and advise relevant members of staff as necessary to avoid the same or similar complaints arising in the future.

14.3 The number and type of complaints received will be reported to the Audit Committee on a termly basis, within the termly and annual GDPR reports.

15. Implementation and Review

15.1 This procedure will be reviewed from time to time, and at least every two years, to ensure that its provisions continue to meet the College's legal obligations and reflect best practice.

16. Right To An External Review

16.1 If a complainant remains dissatisfied after they have received the response to their complaint, they have the right to refer the matter to the Information Commissioner's Office (ICO) at https://ico.org.uk/ or at 0303 123 1113.