



## Data Protection Complaints Policy and Procedure

### 1. INTRODUCTION

This policy sets out how Norland provides a clear, fair and accessible process for individuals to raise concerns about how their personal data has been handled. It reflects statutory obligations introduced by the UK Data (Use and Access) Act 2025 (DUAA), which requires all organisations to operate an internal data protection complaints process. Complaints must be handled internally before they can be escalated to the Information Commissioner's Office (ICO).

Where personal data has not been handled appropriately, an individual has the right to raise a complaint using various routes. Norland will send an acknowledgement to the complainant within 30 days, conduct an investigation into the complaint and provide progress updates where the complaint is complex. Norland will respond to all complaints in writing.

Where the complainant is dissatisfied with the outcome of the complaint, they may raise it with the ICO.

#### 1.1 Purpose

The purpose of this policy is to outline Norland's framework for receiving, assessing, managing and responding to data protection complaints. It ensures that complaints are handled in a manner that is impartial, timely, accessible and compliant with data protection legislation and DUAA 2025.

#### 1.2 Scope

This policy applies to staff, students, placement families, clients, directors, contractors and third-party processors who process personal data on behalf of Norland.

#### 1.3 Principles

- **Accessibility:** Clear and visible routes for complaints, including emails, post and online forms.
- **Timeliness:** Acknowledgement within 30 days and outcomes provided without undue delay, as required under DUAA Section 103.
- **Fairness:** Impartial assessment of the issues and appropriate enquiries proportional to risk.
- **Transparency:** Clear expectations of findings and actions.
- **Learning:** Complaints inform improvements to data protection practices.

#### 1.4 Definitions

##### Data subject

The living individual to whom the data belongs. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.



|                                          |                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personal data</b>                     | Any information relating to an identifiable individual i.e.: someone who can be identified either directly or indirectly from that information. This may include details such as a name or address, as well as online identifiers like an IP address. Further guidance on what constitutes personal data is available from the ICO ( <a href="#">What is personal data?   ICO</a> ). |
| <b>Encryption</b>                        | The process of encoding a message or information in such a way that only authorised parties can access it.                                                                                                                                                                                                                                                                           |
| <b>Confidential information</b>          | Information provided by an individual in confidence, which they would reasonably expect not to be shared without their consent or an appropriate legal or organisational exemption, and which is held by Norland on a legitimate basis. This may include medical information, demographic details, and information relating to third parties.                                        |
| <b>Information Commissioner's Office</b> | The ICO is an independent regulatory body responsible for upholding information rights in the public interest. Where an organisation fails to comply with data protection legislation, the ICO has the authority to pursue enforcement action, including criminal prosecution.                                                                                                       |
| <b>Data (Use and Access) Act 2025</b>    | The DUUA 2025 updates legislation relating to digital communication and data protection, supporting innovation and economic growth while safeguarding individuals' rights. It builds on the UK GDPR framework and introduces measures to modernise data governance. The Act also seeks to maintain alignment with EU standards.                                                      |
| <b>Data protection complaint</b>         | A concern raised by an individual regarding how Norland has processed, shared, stored, or protected their personal data, or in relation to the handling of a data subject rights request.                                                                                                                                                                                            |

## 2. POLICY

### 2.1 What individuals can complain about

Complaints may be about:

- The handling of a data subject rights request;
- Suspected unlawful processing, sharing, retention or collection of personal data or;
- Data security concerns or personal data breaches.

Complaints that fall outside of the data protection framework include:



- General service complaints;
- Freedom of Information or Environmental Information Request matters and;
- Issues unrelated to personal data.

These complaints will be referred to the appropriate procedure.

Other reasons why a complaint may not be accepted are:

- The complaint is manifestly unfounded or excessive;
- Duplication of an existing complaint;
- The matter occurred more than three years after the individual became aware of the issues (statute of limitations);
- No valid authority is provided when a representative acts on behalf of a data subject and;
- Norland is asked to access a third-party online portal to respond (this is not accepted).

## **2.2 Time limits**

Individuals are encouraged to submit complaints within 12 months of becoming aware of the relevant issues. Complaints received after this period may still be considered where it is reasonable and appropriate to do so. This approach recognises that, over time, it may become more difficult to obtain reliable evidence and supporting records.

Norland reserves the discretion to investigate complaints relating to events that occurred more than 12 months prior, where it is appropriate to do so. Matters outside this timeframe may be considered, for example, where:

- There is ongoing risk of harm;
- There are safeguarding concerns;
- There is evidence of systematic failure;
- Relevant records or evidence remain unavailable, for example, in CRM systems retention periods have expired.

This ensures that serious concerns are not excluded solely because of the passage of time.

## **2.3 Complaints made on behalf of another person**

Complaints may only be made about the data subject's own personal data unless valid legal authority is provided, including:

- Lasting power of attorney;
- Court Order;
- Parental responsibility or;
- Signed consent or written authority to act.

Norland will not access complaints submitted via a third party or that requires it to click on a link.

## **2.4 Escalation to the ICO**

Following an investigation conducted by a nominated individual at Norland, the outcome will be considered final. If the complainant remains dissatisfied after receiving a full and comprehensive



response, they have the right to refer the matter to the Information Commissioner's Office ([www.ico.org.uk](http://www.ico.org.uk)).

## **2.5 Non-compliance**

Failure to comply with this policy may result in:

- Non-compliance with statutory requirements (DUAA 2025, UK GDPR, DPA 2018);
- Regulatory action by the ICO;
- Reputational and financial damage and;
- Reduced public trust.

## **3. PROCEDURE**

### **3.1 Making a complaint**

Data subjects and third parties may make a complaint relating to Norland's use of personal data. Complaints should be sent to the Pro Vice Chancellor (PVC) (HR & Compliance) at [NorlandHR@norland.ac.uk](mailto:NorlandHR@norland.ac.uk). Complaints will normally be acknowledged within 30 working days. Norland reserves the right to extend the period we need to respond during vacation and university closure.

Although a complaint may be brought at any time, there may be limit as to what Norland can do in historic cases.

Norland will only accept a complaint from a data subject's representative, if the representative provides the data subject's written consent authorising the representative to act on the data subject's behalf in relation to the complaint.

If there is any doubt about the identity of the complainant, the PVC (HR & Compliance) will first seek to verify the data subject's identity or third party's entitlement to act on behalf of the individual. The forms of identification that are acceptable from a data subject are as follows:

- Passport
- Driving licence
- For third parties, the identification requirements will vary depending on the relationship with the data subject. These will therefore be assessed on a case-by-case basis.

### **3.2 Investigation and complaint outcome**

Once all identification requirements have been met, the investigation will be carried out normally within the 30 working days acknowledgement period. If further clarification is required from the complainant or more time is required for the response to be completed, Norland will inform the complainant prior to the original deadline.

The complaint outcome will be communicated to the complainant in writing, normally by email.



### **3.3 Review**

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 Vice Chancellor. The decision will be internally reviewed by the Vice Chancellor normally within 20 working days from the receipt of the request for Review.

Once the internal review has been completed, Norland will communicate the outcome in writing, normally by email.

### **3.4 Escalation to the Information Commissioner's Office**

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

The complainant does not need to complete the internal review stage before escalating their complaint to the ICO. They may do so after receiving the original complaint outcome.

Information about how to make a complaint to the ICO can be found at [Make a complaint | ICO](#).

In order to respond to the complaint, the PVC (HR & Compliance) will investigate the complaint based on the information provided by the ICO. This may necessitate access to personal data and other information held across Norland. The cooperation of any staff members able to assist with the investigation will be required. The reason for the investigation may need to be disclosed to the relevant staff members. The PVC (HR & Compliance) will draft and submit a response to the ICO in consultation with the Vice Chancellor.

In the absence of the PVC (HR & Compliance), the Vice Chancellor will appoint another member of the Strategic Leadership Team to carry out the investigation and respond to the ICO.

### **3.5 Manifestly unfounded, abusive, vexatious or excessive correspondence and complaints**

In some cases, we can refuse to handle 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:

- The data subject has explicitly stated that they intend to cause disruption (whether in the complaint or in other correspondence) and has threatened individuals;
- The data subject has made unsubstantiated accusations against individuals and is persisting in those accusations;
- The data subject is targeting particular individuals against whom they have a personal grudge;
- The data subject makes frequent complaints intended to cause disruptions and;
- The data subject continues to repeat the substance of previous complaints which have already been investigated.



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

- The reasons for refusing to consider the complaint;
- Their right to make a complaint to the ICO and;
- Their right to pursue their data subject rights through a judicial remedy.

### 3.4 Use of data from complaints

Norland will collect data on complaint outcomes at each stage of this procedure and any complaints submitted to any regulators, including the ICO, and use the data internally for reporting, evaluation, learning and training and externally for discussion with regulators.

The data used by Norland for the purposes set out in the above paragraph will be anonymised. Personal data and sensitive personal data as defined by the Data Protection Act 2018 may be disclosed to members of staff and regulators only for the purpose of dealing with complaints, or a complaint arising out of it and/ or implementing any recommendations. Personal data will not be shared with any other third parties unless Norland has the explicit consent of the complainant. Has a statutory obligation to do so or is otherwise permitted to do so under the DPA.

## 4. MONITOR AND REVIEW

Responsibility for ensuring compliance with this policy and procedure rests with the PVC (HR & Compliance). The policy will be reviewed every two years, or sooner if required in response to legislative or regulatory changes.

| Document Control Information                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy title:</b>                                              | Data Protection Complaints Policy and Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Summary description:</b>                                       | This policy sets out Norland's approach to handling data protection complaints in accordance with the UK Data (Use and Access) Act 2025 (DUAA). It provides a clear, fair and accessible process for individuals to raise concerns about the handling of their personal data, ensuring complaints are managed impartially, transparently and in compliance with data protection legislation. The policy outlines who may make a complaint, the types of issues that can be considered, the process for investigation and review, and the circumstances in which complaints may be escalated to the Information Commissioner's Office (ICO). It also establishes timescales for responding to complaints, the requirements for complaints made on behalf of others, and Norland's commitment to using complaint outcomes to strengthen data protection practices and maintain regulatory compliance. |
| <b>Relates to staff/ student (include Set), NQN or Norlander:</b> | All users                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Version number:</b>                                            | V1.0/ST/14092026                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



|                                   |                        |
|-----------------------------------|------------------------|
| <b>Owner:</b>                     | PVC (HR & Compliance)  |
| <b>Housekeeping updates only:</b> | New policy             |
| <b>Approving body:</b>            | SLT                    |
| <b>Related Norland documents:</b> | Data Protection Policy |
| <b>Date of approval:</b>          | 14 September 2026      |
| <b>Date of effect:</b>            | 16 September 2026      |
| <b>Frequency of review:</b>       | 2 years                |
| <b>Date of next review:</b>       | September 2028         |
| <b>Upload to website:</b>         | Yes                    |