Data Protection Policy

1. INTRODUCTION

Norland College (Norland) is committed to complying with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) (together, the Data Protection Legislation) as an academic institution, an employer and as a service provider. This document outlines the framework that Norland has in place to ensure compliance with Data Protection Legislation.

Any references to staff include all staff working for Norland (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, the Board of Directors, contractors, volunteers and temporary staff.

2. POLICY

Norland helps to ensure compliance with data protection law using the measures outlined below.

2.1 Training and awareness

Norland is committed to ensuring all staff have the requisite training and awareness around data protection. All staff must undertake the compulsory core training module as part of their induction programme and refresher training is provided every two years. The training is online and staff must pass a test to complete the training.

The training includes (but is not limited to) the practical application of the UK GDPR's principles, guidance on how to keep personal data secure and when staff should speak to the Head of HR, Resources and Compliance (Head of HRRC).

The Head of HRRC attends external training which is appropriate to their role as the senior individual who leads on Norland's data protection compliance.

Breaches of data protection law due to unauthorised access, misuse, negligence or loss may result in disciplinary action, up to and including dismissal.

2.2 Documentation

Documenting how we comply with Data Protection Legislation is a key part of our compliance. In addition to the documents listed above we:

- maintain a record of how we use personal data as required under Article 30 of the UK GDPR. The Head of HRRC is responsible for maintaining this record;
- document our lawful bases for using personal data through our privacy notices;
- keep a record of our legitimate interests assessments;
- carry out risk assessments and when required a Data Protection Impact Assessment;
- retain records of any consents obtained to use personal data;
- maintain a register of any data breaches. The Head of HRRC is responsible for completing this. All staff understand that they must inform the Head of HRRC of any suspected breach so that the register can be kept up to date;

- record when staff complete data protection training to ensure that all staff have received the appropriate level of training; and

- maintain an appropriate policy document regarding our processing of special category personal data and criminal offence data as required by the DPA 2018.

2.3 Privacy Notices

Norland has privacy notices, which are published on Norland's website.

In addition, Norland explains how personal data will be used on a case by case basis as appropriate. For example, forms that are used to collect personal data will include a brief description of how and why it will be used, and cross refer to the applicable privacy notice.

2.4 Data protection by design and default

Norland has built the data protection principles into its practices by implementing appropriate technical and organisational measures. This is known as data protection by design. The UK GDPR sets out seven key principles which are at the heart of Norland's approach to processing personal data, and which are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

We also ensure that we only use the minimum amount of personal data to achieve our purposes - known as data protection by default.

More specifically we do the following:

- at the start of any new project, or new activity, which involves using personal data (e.g. working with a new external provider, implementing new software or hardware), we consider how we will comply with the data protection principles and whether we need to carry out a Data Protection Impact Assessment (DPIA) to identify privacy risks and plan appropriate mitigation. Further information regarding DPIAs can be found on SharePoint;

- we make it clear on any data collection forms what personal data must be provided and what is optional;

- we proactively consider data protection risks and adopt appropriate measures to protect personal data (e.g. encryption, physical security);

- our external facing documents (e.g. privacy notices) are accessible;
- before we share personal data externally we check that we have a lawful basis and that the sharing is fair;
- we regularly review the measures which are in place to ensure that they are still appropriate;
- we have developed a culture where staff understand the importance of data protection; and
- if there has been a problem, or a "near miss", we will look at what has happened to improve our practices, for example, by providing additional staff training and awareness.

Norland has various internal written procedures in place to comply with our obligations under the UK GDPR. This includes in relation to:

- computer and network security;
- the secure destruction of personal data - both electronic and paper copies;
- individuals exercising their rights;
- ensuring that we only use processors who comply with the UK GDPR; and
- physical security when Norland site is used by external parties.

2.5 Rights

We are committed to allowing individuals to exercise their rights under the UK GDPR. These rights are as follows:

Right	**Context for Norland College**
Right of access (subject access requests)	Data subjects have the right to ask what information Norland holds about them and to be provided with a copy of it. This is commonly known as making a subject access request. Norland will also give data subjects extra information, such as why Norland uses this information about them, where it came from and who Norland have sent it to.
Right to rectification	Norland makes every effort to ensure data is accurate. If information we holds about a data subject is incorrect or incomplete, the data subject can ask Norland to correct it.
Right to erasure / right to be forgotten	Data subjects have the right to ask Norland to delete the information that it hold about them in certain circumstances. For example, where it no longer needs the information.
Right to restriction of processing	Data subjects can request that Norland restricts how it uses their personal data in certain circumstances.
Right to data portability	Data subjects have the right to request the transfer of their personal data to themselves or to a third party in a format that can be read by computer. This applies where (a) the information has been provided by the data subject; (b) the basis that Norland are relying on to

	process their personal data is consent or contract; and (c) the information is being processed electronically e.g. on a computer.
Right to object to processing	Data subjects may object to Norland using their personal data where: (a) Norland are using it for direct marketing purposes; (b) the lawful basis on which Norland is relying is either legitimate interests or public task; (c) if Norland uses their personal data for scientific or historical research purposes or statistical purposes.
~~Automated decision making, including profiling~~	~~Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.~~

Staff are trained to recognise when an individual is exercising a right under the UK GDPR and to pass this immediately to the Head of HRRC.

Norland keeps a log of all requests to exercise rights with the applicable deadline for our response. This log is maintained by the Head of HRRC.

To ensure that we meet our obligations the Head of HRRC co-ordinates our response to all requests. The Head of HRRC has detailed knowledge of how to respond to individuals' rights. The Head of HRRC will involve other members of staff, as appropriate, in formulating Norland's response.

Consideration is given to at least the following issues when responding to rights requests:

- the importance of responding within the statutory timeframe, usually one calendar month (but this can be extended by up to two months for complex requests);
- whether further engagement with the requester is needed, e.g. to ask for ID, check authorisation given for a third party to make the request on their behalf or to seek clarification of their request;
- the exemptions under the Data Protection Act 2018;
- the provision of supplementary information (e.g. sources and purposes) under a subject access request;
- whether the request can be refused, or a reasonable fee charged, because it is manifestly unfounded or excessive; and
- how to securely send our response to the requester.

2.6 Security

Norland has put in place technical and organisational measures to ensure the confidentiality, availability and integrity of personal data. The Principal is responsible for determining the appropriate organisational measures, for example, staff training and guidance, and this is delegated on a daily basis to the Head of HR, Resources and Compliance.

The Vice Principal leads on the technical side of our information security, for example, network security. Norland follows guidance from the National Cyber Security Centre and keeps up to date with the latest cyber security news and alerts.

Norland has implemented an IT Security Policy and ICT Acceptable Use Policy for staff. Details of the IT Security Policy and ICT Acceptable Use Policy can be found on SahrePoint.

We appreciate that prompt action is vital when handling information security incidents. Staff are trained to report any suspicions or concerns regarding potential personal data breaches to the Head of HRRC immediately.

The Head of HRRC will carry out an initial investigation and determine if the incident constitutes a personal data breach. If so, the procedure outlined in Norland's personal data breach procedure will be followed.

2.7 Data sharing

Norland will only share personal data with third parties where it is lawful, fair and transparent to do so, and in accordance with the other requirements under Data Protection Legislation. Norland will ensure that it has identified a lawful basis in order to share the personal data.

2.8 Using data processors

Norland may use an external contractor or 'data processor' to process (e.g. store) its data. The data processor will process data only for the purposes specified by Norland and will be bound by a contract which includes the specific terms required by the UK GDPR. Where data is passed outside the UK, Norland will take the relevant steps to ensure there is adequate protection in place in accordance with Chapter V of the UK GDPR.

Norland has procedures in place to check that organisations acting as our data processors are complying with the UK GDPR. The Vice Principal and Head of HRRC are responsible for implementing these procedures.

Staff are trained to speak to the Head of HRRC if they need to share information with an organisation which may act as Norland's data processor so that the Head of HRRC can check that the appropriate measures are in place.

2.9 Academic research

Academic research which involves the processing of personal data is subject to the Data Protection Legislation. All academic projects are subject to the Research Ethics Handbook, which includes specific directions for projects involving personal data. The Research Ethics Handbook can be found on SharePoint.

2.9 International transfers

Norland maintains a record of when it transfers personal data outside of the UK and what safeguard or derogation is relied on under the UK GDPR. This is logged in the CRM database used by the employment agency.

2.10 Data Protection Fee

Norland is registered on the Information Commissioner's Office's (ICO) register of fee payers under registration number: Z8065825.

Norland has procedures in place to ensure that the data protection fee is paid to the ICO and the Head of HRRC is responsible for ensuring that the fee is paid on time.

2.11 Monitoring and review

Any personal data breaches at Norland will be followed by a review of the relevant procedures by the Head of HRRC and a report made to the Senior Leadership Team and Audit Committee.

The Head of HRRC will ensure that the content and implementation of the procedures set out in this policy are reviewed regularly.

3. ROLES AND RESPONSIBILITIES

The Head of HR, Resources and Compliance has been appointed as the Data Protection Lead. The Head of HRRC is responsible for managing Norland's compliance with Data Protection Legislation. The Principal has ensured that the Head of HRRC has sufficient time and resources to fulfill their tasks.

The Head of HRRC regularly reports to the Audit Committee who are responsible for Norland's data protection compliance. Data protection is a standing item on the agenda at the audit committee meetings.

All staff have a role to play in Norland's data protection compliance. Staff are encouraged to ask questions and raise concerns with the Head of HRRC or their head of department. This allows Norland to regularly review and strengthen the data protection measures we have in place.

4. RELATED POLICIES, PROCEDURES AND GUIDANCE

All staff at Norland are required to comply with the following documents:

- A Practical Guide for Staff - Data Protection
- IT Security Policy; and
- ICT Acceptable Use Policy;

The Head of HRRC] and Senior Leadership Team are responsible for implementing the:

- Data Breach Policy and Procedure;
- Data Retention Policy and Schedule;
- CCTV Policy; and
- Appropriate Policy Document for special category personal data.

Document Control Information	
Policy title:	Data Protection Policy
Version number:	V1.0/ST/01092024
Owner:	Head of HR, Resources and Compliance
Approving Body:	SLT
Related Norland Documents:	A Practical Guide for Staff - Data Protection IT Security Policy ICT Acceptable Use Policy Data Breach Policy and Procedure; Data Retention Policy and Schedule CCTV Policy Appropriate Policy Document for special category personal data.
Date of approval:	September 2023
Date of effect:	September 2023
Frequency of review:	2 years
Date of next review:	September 2025