



Employee Privacy Notice

Norland College is committed to protecting your personal and sensitive data, working in accordance with current data protection legislation. This privacy notice outlines how Norland collects, processes and uses your personal data. This privacy notice is applicable to all employees (current, past or prospective) and other colleagues who have a temporary or ongoing association with Norland, including Directors and Trustees.

Why we collect your personal data

Norland collects personal data in order to fulfil its obligations as an employer. There is always a lawful basis for processing your personal data including, but not limited to, the performance of an employment contract and compliance with Norland's legal obligations, which are outline below.

Norland will not process personal data for marketing purposes and it is not subjected to automated data processing.

It is important that your personal data is kept current and is accurate. Please ensure you inform HR as soon as possible should your personal information change.

The types of information we collect

The following are examples of personal data which may be collected, processed and stored by Norland. This list is not exhaustive.

- Personal contact details (name, date of birth, address, telephone numbers, personal email addresses)
- Next of kin and nominated emergency contact information
- National insurance number, bank account details, payroll records and tax status information
- Salary, pension and benefits information
- Absence records, Fit for Work notes, medical reports
- Information about your health, including any medical condition and/ or disability information
- Copy of passport and driving licence
- DBS disclosure number, information about criminal convictions and offences
- Marital status and dependents
- Information relating to protected characteristics
- Recruitment information (application form, CV, letters, references, copies of right to work documentation)
- Employment records (job titles, contract of employment, conflicts of interests, work history, working hours, training records and professional memberships)
- Compensation history (allowances and bonus payments)
- Salary benchmarking and pay modelling
- Staff Development Review information including personal development information
- Disciplinary, grievance and performance management information
- Information relating to maternity, paternity, shared parental or adoption leave and/ or pay

- CCTV footage and other information obtained through electronic means such as swipe/identity card records
- Information about your use of our information and communication systems
- Photographs

Norland will collect your personal data in different ways prior to and during its working relationship with you. These will include:

- Information provided as part of the application and/ or recruitment process
- Information provided as part of your period of employment with Norland

How Norland uses your personal data

Norland requires staff to share their personal data in order to manage the employment relationship. Examples of how Norland may use your information are as follows:

- Recruit and select new and existing employees, temporary workers and consultants
- Pre-employment checks relevant to the role appointed to
- Administer employment contracts for all staff including fixed term, term time only and student helpers
- Maintain accurate information for all current staff in the HR database (CascadeGo)
- Pay wages and benefits, including pensions and expenses, to which they are entitled to and that the necessary deductions are made eg: tax, student loan repayments, etc
- Manage the health and well-being of staff through maintenance of emergency contact details, pre-employment medical details, health screening for relevant roles, information related to disability, incident records, Personal Emergency Evacuation Plans (PEEPs), personal risk assessments and staff survey monitoring, etc
- Record staff absence including sickness, dependents leave, parental leave, jury service, etc, and maintain absence management procedures for effective workforce management and employee well-being ie: fitness to work and reasonable adjustments
- Record and monitor staff performance, training, development and career progression
- Operate and keep a record of disciplinary, grievance and other employee relations processes
- Report and monitor data relating to protected characteristics to inform and develop plans to promote equality, diversity and inclusion at the recruitment stages and within the workplace
- Process specific reports and returns and participate in general statistical surveys for governmental or regulatory bodies such as pension providers, HMRC, HESA, of the Office for Students
- Facilitate internal operational communications relevant to your employment with the College and promotion of your work details on the staff intranet (MyDay) and Norland's website. This also covers managing security through photographic staff ID cards
- Fulfil and monitor legal responsibilities and obligations, for example immigration, health and safety and the Prevent duty
- Provide references on request for current and former employees
- Provide relevant management information to support the College with effective financial forecasting, workforce management and business planning
- Support staff with making applications for research or other funding and regulatory approvals
- Support teaching and learning and staff development with audio or video recording of lectures, presentations or training events

The lawful basis for processing personal data for employees

The College processes staff data for the above purposes in order to:

- Fulfil its obligations under the contract of employment
- Be legally compliant
- Protect the vital interests of staff, for example in the case of a medical emergency
- Perform a task carried out in the public interest

The College will only process special category data with the explicit consent of the member of staff involved or under the following conditions:

- For the member of staff and/or the College to carry out their employment obligations providing that appropriate safeguards are in place to protect the individual's fundamental rights and interests
- For the establishment, exercise or defence of legal claims
- To protect a member of staff's vital interest when they are incapable of giving consent, for example in a medical emergency
- For reasons of substantial public interest
- Archiving purposes in the public interest, historical or statistical purposes

If your consent is required for any specific use of your personal data, it will be requested and collected at the appropriate time.

Accessing employee data

Employee personal information is held by the Human Resources department. All personal data is carefully controlled with restricted access. Only those staff who have a legitimate business requirement will be granted access.

Other possible reasons for accessing your personal data are as follows:

- For operational and business continuity purposes, your personal data may be shared with other relevant members of staff including senior management
- For sharing across relevant IT systems and databases to facilitate the management and delivery of Norland's services, legal requirements
- Finance require to certain personal information for effective forecasting and to process BACs payments eg: wages, expenses
- Line managers will have access to certain personal information through CascadeGo to fulfil their obligations as your line manager
- Senior managers have access to certain personal information following incident reports to enable them to fully investigate those incidents and ensure appropriate control measures are in place

Norland takes your privacy and the security of your personal data very seriously. Requests to access your data are only approved if there is a legitimate reason which is covered by the relevant lawful basis. Your consent will be sought, it will be requested and collected in advance of your information being shared.

Third party sharing

The College will disclose certain personal data to external parties for the legitimate interests of the College and/ or third parties as follows:

| External / Third party | Details and legitimate grounds for processing |
|--|--|
| Disclosure and Barring Service (DBS) and U-Check, the online counter-signatory umbrella body who processes the DBS applications on the College's behalf. | Pre-employment check; contributes to ensuring the suitability of the successful candidate to a particular position where DBS clearance is required. |
| HMRC | For the collection of income tax and national insurance contributions from employees. |
| Pension providers: Teachers' Pension Scheme and Scottish Widows. | To allow provision of pensions by these providers. |
| Third party software suppliers. | Where external computer systems are used, for example CascadeGo, there may be occasions where access is granted to ensure operational management. A formal agreement will be entered into by the third party and the College to protect employee data. |
| Third party payroll provider. | To provide payroll services. |
| Audit companies. | To enable internal/ external audit / investigation. |
| Third party IT supplier. | Oversee all internal network drives and servers. |
| Publicly available on the website. | To enable effective communication, certain information is included on the College's website eg: name, photograph, work contact details, biographies, committee membership, etc. |
| Office for Students. | To support the requirement for statistical returns and demonstrate compliance with OfS regulations. |
| Mortgage companies and letting agencies. | For mortgage and letting verification purposes. Information will only be disclosed with the written consent of the employee. |

Retention of personal data

Your personal data will be kept as long as necessary for the purposes(s) for which it was collected. Please view the College's Retention Schedule for further information. All personal data will be securely destroyed when no longer required.

Employee data subject rights

As a data subject, you have the following rights with regards to your personal data:

- Access and obtain a copy of your data on request
- Request the College amends incorrect or incomplete data
- Request the College to stop processing your data
- Object to the processing of your data where the College is relying on its legitimate interests as the legal grounds for processing
- Request that the College erase all your personal data
- Request the College restricts its data processing activities and, where the College's processing is based on your consent, you may withdraw that consent, without it affecting the lawfulness of processing based on consent before withdrawal

- Receive from the College the personal data held about you which you have provided, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller

Please note that the above rights are not absolute and the College may be entitled to refuse requests where exceptions apply.

If you wish to exercise any of these rights, or if you have a complaint about the way your data is being processed, please email privacy@norland.ac.uk in the first instance.

If you have a complaint and you remain dissatisfied with how your complaint has been dealt with, you can take your complaint to the Information Commissioner's Office (ICO) at casework@ico.org.uk

Changes to this notice

This privacy notice is reviewed annually or when required, to ensure compliance with data protection legislation.

Reminder of individual's responsibility

Individuals also have a responsibility for the security of their personal data. Please remember the College will never ask you to share your username and password nor should you share them with another. For further information and guidance on information security, please follow [this link](#).