

Staff Privacy Notice

Your personal information

The University of Lincoln is registered as a data controller with the Information Commissioner's Office for the purposes of relevant Data Protection legislation.

The University of Lincoln holds and processes personal data and special category data about its current, past, and prospective staff and others who are defined as data subjects. This information is normally provided to the University by a prospective employee when applying for a vacancy and is added to by the University over the course of employment. Information about staff and prospective staff is retained and disposed of in accordance with the University's Data Retention Policy. Some information may be archived securely to enable compliance with legislation in relation to employment after the engagement has ceased.

This privacy notice applies to all individuals under an employment contract and for those engaged under an honorary contract of employment.

Personal Data

Personal data is data relating to a living individual who can be identified from that information or from that data and other information in the University's possession. E.g., name, address, telephone number. It can also include expressions of opinions about an individual. E.g., interview notes made by a panel member.

Special Category Data

Special Category data relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life, sexual orientation, genetic data, biometric data where processed to uniquely identify a person.

The University needs to process certain personal data about its staff for several administrative purposes. The legal bases for processing data are:

Necessary for the performance of a contract

- Managing Human Resources processes such as recruitment, payment of salaries and pensions, performance management, administering benefits, and training and development.
- Providing communications about University news and events.
- Providing facilities such as ICT services, Library services, and car parking provision.
- Accessing University spaces when using a staff ID card (via the Salto Access Software).

Necessary in order to comply with a legal obligation

- Compliance with legal obligations such as making external / statutory returns to the Higher Education Statistics Agency (HESA).

- Monitoring equal opportunities.
- Office for National Statistics (ONS) Returns.

Necessary for the University to perform a task in the public interest

- Provision of wellbeing and support services.
- Managing a safe working environment under the relevant health and safety legislation. For example, contacting employees using their personal contact details when home-working to update them with appropriate information.
- Maintaining contact with past employees.
- Publishing lecture recordings in support of the University's public task of providing higher and further education, and to the extent that any special category data would be processed (e.g., ethnicity, health-related discussion) this is done on the legal basis of substantial public interest. Staff remain free to opt out of lecture recording/publishing should they object to it.
- Security team using body-worn cameras to record incidents that help prevention and detection of crime, safeguarding staff and visitors, and ensuring compliance with health and safety procedures. Please note these cameras are only switched on when responding to an incident. I.e., not during routine patrolling.

The University processes special category data for several administrative purposes. The legal bases for processing data are:

Necessary for the performance of a task carried out in the public interest

- **Monitoring the existence of absence of equality of opportunity or treatment between groups of individuals.**
 - Monitoring equal opportunities.
 - Managing a safe environment and ensuring fitness for work.
 - Managing obligations under Equal Opportunities legislation.
 - Provision of occupational health and wellbeing services to individuals.
- **Necessary for the assessment of the working capacity of an employee**
 - Managing Human Resources processes such as administering Sick Pay and Sick Leave schemes, managing absence, administering Maternity Leave and related pay schemes.

This notice explains more about how we use your personal information.

- What information we collect about you
- How we use your information
- Information we may share with other organisations
- Information processed abroad
- How long we keep your information
- Accessing your information and other rights
- How to object or withdraw consent
- How to contact us
- How to complain

What information we collect about you

The University will process your information in accordance with relevant Data Protection legislation. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely, be adequate, relevant and not excessive, be kept accurate and up-to-date, held only as long as necessary, and not disclosed to any third party unlawfully.

Any breach of relevant Data Protection legislation is considered to be an offence, and in that event, the University disciplinary procedures will apply.

We collect information about you when you initially applied to work at the University of Lincoln. Further information was then sourced if you were successful in obtaining the role.

- Identification data (e.g., name, personal address, personal telephone numbers, personal email address, date of birth, national insurance number, emergency contact information)
- Information concerning employment (e.g., salary, work and pay history, performance information, job applications, active military reservist dates)
- Financial information (e.g., bank account details, salary-related information)
- Special Category information (e.g., information which may reveal race or ethnic origin for employment equality purposes, religious beliefs, disability, sexual orientation)
- Other information necessary for the University's business purposes which may be voluntarily disclosed by individuals to the University during an employment with the University.

Employees can keep their details up to date by using the HR online self-service software, MyView. Where specific elements of data are not amendable, or available on MyView, contact the Human Resources department (hr@lincoln.ac.uk)

How we use your information

Within the University, personal data may be shared between colleagues who legitimately need the information to carry out their duties.

Your personal contact details may be shared with relevant colleagues to communicate urgent health and safety information to you.

To set up multifactor authentication (MFA) for staff account security, personal email addresses (if provided as an applicant at the point of recruitment) may be used as a verification method.

Upon creation of a staff email account, an employee's name, school / department, email address, and telephone number will appear in the University's internal staff directory. This information may also appear on externally facing University web pages.

Staff photographs are used on University Staff Cards for the purposes of identification and security.

Some information (name, email address, workplace location, department/school, and telephone number) is passed to the University's Computer-aided facility management (CAFM) system for the purposes of making maintenance requests. This allows relevant University staff to contact other staff to pass on updates in relation to these requests. Location data is used to enable the University to communicate any disruptive or high impact works taking place in the buildings employees are located in.

The University may monitor computing use to ensure adherence to the University's Acceptable Usage Policy or for statistical purposes.

The University has enabled lecture recording in all its centrally timetabled teaching spaces. These recordings are lecturer initiated, and access to recordings is controlled via the *Panopto* software. To manage student expectations, staff should inform students when lecture recording will and will not be used. Typically, this should be done at the start of a new module when teaching and assessment approaches are introduced and included in relevant documentation. Staff should also liaise with colleagues within the programme to

ensure consistency in approach. To assist yearly housekeeping and avoid inadvertent erasure, all lecture recordings will be deleted on academic request at the end of each academic year (normally September). Requests should be submitted to the Digital Education Team. This practice is to enhance the student experience by providing them with supplemental support that puts inclusivity and alternative access at the core, and therefore proactively supports Equality and Diversity, and support for all support outcomes. Staff remain free to opt out of the lecture recording/publishing should they object to it.

The University is required to obtain information about past criminal convictions as a condition of employment for certain posts. The University also undertakes Disclosure and Barring Service (DBS) checks on those staff who work with young and/or vulnerable people.

To support the real-time integrations between systems a middleware platform may be used. In the case of the University of Lincoln this is provided by Microsoft BizTalk Server. As such, any data which passes through said middleware will be secured by in-transit encryption using the technologies provided and whilst the data is being “processed” is deemed to be in flight. During this process, the data is only visible for split second whilst the middleware solutions carry out internal data mapping to ensure downstream systems receive the required data. For clarity, the data which is in-transit isn’t stored and only passes through a BizTalk message box for routing purposes. The main contribution of this methodology consists in identifying the information system, and not the processing per se, as the object of the analysis due to the complexities of the processes involving personal data. To this end, the University of Lincoln ICT department will periodically review the data requirements to ensure that any downstream systems are providing creation, updating of records and deletion processes in accordance with the GDPR policy. No downstream systems will hold any data relating to a student who has left the University unless this is for the purposes of debt collection or supporting the collection of outstanding ongoing payments.

The amount of personal information shared within the University will be no more than is reasonably necessary.

The University occasionally uses cookies and other technologies on its website that collect data about you when you use them. Where this occurs, further information will be available in a cookies policy. The cookies policy for the University website can be found here: <http://www.lincoln.ac.uk/home/termsconditions>.

Information we may share with other organisations

The University may need to share your personal and special category data with third parties outside of the University who are contracted to work on its behalf. For example, to Travel Management Companies, pension providers, insurers or legal consultants.

The University has a legal obligation to disclose staff personal data to the Office for Students (OfS) and the Higher Education Statistics Agency (HESA) and/or their nominees/successors. HESA will process your information in accordance with their collection notice.

If your contract is a joint contract (e.g., with the NHS) or you are on secondment, then certain information will be shared with the host / honorary employer in accordance with your contract.

The University may also have to share your personal data with third parties outside the University for other purposes with your consent. However, there may be circumstances where information is shared without consent. This will only be if:

- The disclosure is in the legitimate interests of the University.

- There is a statutory obligation to share the data. E.g., for making returns to the local authority, to the Office for Students (OfS), to the Higher Education Statistics Agency (HESA).
- There is a legal obligation to share the data. E.g., when submitting the yearly Annual Survey of Hours and Earnings (ASHE) return to the Office for National Statistics.
- Disclosure is required for the performance of a contract.
- Disclosure is necessary to protect your vital interest. E.g., in a medical emergency.
- Disclosure is made to assist with prevention or detection of crime, or the apprehension or prosecution of offenders.
- Disclosure is required by a Court Order.
- Disclosure is necessary to assist the University obtain legal advice.

Pension Providers

East Riding of Yorkshire Pension Fund
 Teachers' Pension Scheme
 Universities Superannuation Scheme
 People's Pension Scheme
 University and Colleges Retirement Savings Scheme (UCRSS)
 NHS Pension Scheme

Information is shared in relation to contact details and contributions and in compliance with pension legislation including the Pensions Act and Auto Enrolment. This data is processed to ensure the accurate administering of the pension scheme and the provision of pension forecasts and payments.

Higher Education Statistics Agency (HESA)

Annually, the University has a legal obligation to send anonymised staff data to HESA. Special Category data such as ethnic origin and disability is included in the data set.

Although employees cannot withdraw themselves from being included in the anonymised data set, many fields have the option of using the code description 'prefer not to say' at the point of collection.

The HESA Data Collection Notices can be found on HESA's website (<https://www.hesa.ac.uk/fpn>).

Official for National Statistics (ONS)

Annually, the University has a legal obligation to send personal information to the Office for National Statistics in the form of its *Annual Survey of Hours and Earnings (ASHE)* return. The ONS selects a small sample of employees and asks the University to provide information to them on:

- *Employment Start Date*
- *Job Title*
- *Open-ended / fixed-term contract basis*
- *Basic Pay*
- *Hourly Rate*
- *Number of Hours Worked*
- *Overtime Pay*
- *Overtime Hours*
- *Other Payments Received*
- *Pension Membership*
- *Employer and Employee Pension Contributions*
- *Benefits In Kind Payments*

- *Annual Leave Entitlement*
- *Employment Leaving Date*

ASHE is based on a sample of employees in the United Kingdom and uses the national tax register as its sampling frame. The results of the survey provide an estimate of the levels, distribution and make-up of earnings which are used by Government, employers, and other interested parties.

HM Revenue and Customs and Government bodies

Information is passed to government agencies in relation to allowing them to update employment records and to cross reference employment records with those held on central government systems. Information is passed at the point of each payroll cycle in line with legislative Real Time Information reporting in relation to personal identification, earnings, statutory deductions and working hours.

This information is used to ensure that HMRC can correctly calculate legislative employment liabilities and allocate employment credits to the accrual of state benefits.

UK Border Agency

Information is passed to the UKBA in respect of employment and to ensure compliance with legislation that allows employees to be able to work within the UK.

Information in relation to personal identification, employment commencement and end dates, remuneration and residences may all be passed to the UKBA at their request or in the provision of securing work permits.

University's insurers and legal advisers

In order to ensure compliance with the Corporate Manslaughter Act and the employers Duty of Care details in relation to driving licences and insurance will be collected and held on the University databases for any individual using their own vehicle for University business or where they drive a university provided vehicle via a third party arrangement.

This information will be updated on an annual basis or upon a change to personal circumstances.

Child Maintenance Service, attachment of earnings and Court Orders

The University will pass over information in relation to Attachment of Earnings orders from government bodies. This will be in relation to personal contact details and the remittance of deductions along with the release of employment data for example earnings levels and frequency in relation to ongoing assessment of the deductions to be taken.

Employment start and end dates will be passed to the third parties to update their records as appropriate to the University duties to collect attachments via the University payroll.

Occupational Health Providers

The University's current provider (as of June 2022) is RPS. They process personal details (including special category data). This data may be supplied by the employee, the University, and other health professionals.

Data is retained in accordance with relevant legislation and in line with Records Management Code of Practice for Health & Social Care 2016 (Information Governance Alliance). Clinical records are retained for six years following the last date of entry, or 75th birthday. Statutory records

must be retained for the period specified in the relevant legislation which may be up to 50 years (e.g., Ionising Radiation Regulations).

Third Party
Benefit
Providers

Information is passed to third party benefit providers for the purpose of validating University of Lincoln employees to access and make applications to benefits. Information will be to personally identify an individual as a University of Lincoln employee, and may include employee identifier, surname, and work email address.

This information will be updated on a timely basis to reflect changes to the active workforce or changes to individual personal identifiers.

Third party
system
providers

The University procures third party providers to both hold and process employee data to carry out the employment functions required. These providers cover the provisions of recruitment; employee database; payroll; online learning platforms; and role evaluation.

With all providers, the minimum data to carry out the service is transferred and stored on the third-party platform. All third-party providers perform the required tasks under a University Service Level Agreement (SLA) and Data Processing Agreement (DPA).

All providers receive updates in respect of active employees with leavers of the University being removed from the database or anonymised where data is held for the purpose of equality monitoring or business activity monitoring.

Third party
benchmarking
services –
Universities
and Colleges
Employers
Association
(UCEA) and
XpertHR

To help benchmark the performance of the University against the higher education sector, the University subscribes to two third party benchmarking service providers (UCEA and XpertHR). The lawful basis for processing this information is *Legitimate Interests*. The University completes two annual surveys: the UCEA Senior Staff Remuneration Survey; and XpertHR's Salary Survey of Higher Education Staff. The UCEA survey relates to all senior management employees, and the XpertHR survey refers to all employees below the senior management pay scales.

The University provides UCEA with the following information:

- Job title
- Department
- Sex
- Birth year
- Basic pay
- Other payment allowances (including additional duties, bonus/PRP, responsibility allowance, market forces supplements, and substitution for employer pension contributions)
- Total pay

The University provides XpertHR with the following information:

- Job title
- Date of birth
- Sex
- Basic salary
- Other payment allowances (including market forces supplements, and additional duties)

Surveys are provided to UCEA and XpertHR via encrypted online data transfer tools.

With both providers, the minimum data in order to carry out the service is transferred and stored on the third-party platform. Both third party benchmarking services perform the required tasks under a University Service Level Agreement (SLA) and Data Processing Agreement (DPA).

Information processed abroad

No information provided to the University throughout employment or through the subsequent arrangement with a third party is stored outside of the EEA.

How long we keep your information

- Recruitment information – unsuccessful applicant data will be held within the recruitment system for a period of 1 year before some fields (e.g., names, personal and email) are anonymised for future reporting purposes.
- Payroll data - is held in line with HMRC audit requirements of the current tax year plus the 6 prior years.
- Employment records – are held in line with employment legislation for a period of 7 years post termination.
- Information held in the Computer-aided Facility Management system is archived after one year. Archived records are only visible to system administrators.
- Information held in the Salto Systems Access Control system is archived after one year.

The University will employ reasonable means to keep Employee Personal Information accurate, complete, up-to-date, and reliable for its intended use including prompts for employees to check their information through the employee self-service portal.

If you access additional University services these may keep a record of your contact and will provide you with details of how long they keep your information.

Accessing your information and other rights

You have several rights relating to your personal information. These include:

- | | |
|--------------------|--|
| Access | <p>You have the right to request a copy of any personal information we hold about you.</p> <p>If you would like a copy of any of your information, please contact the Information Compliance team on the details below. The team will process your request within a month.</p> |
| Portability | <p>If you have provided information on the basis of your consent or for a contract, then you can request a digital copy so you can send it to another organisation.</p> <p>To request a copy please contact the Information Compliance team on the details below. The team will process your request within a month.</p> |
| Correction | <p>If any of the information we hold about you is incorrect or incomplete, then please let us know. You have the right to have your information corrected so that we hold accurate records about you.</p> |
| Erasure | <p>This is also known as the right to be forgotten. You can request that your personal information is erased if it is no longer necessary for the University</p> |

to keep it, or you withdraw consent that you have previously provided, or you object and there is no overriding grounds to keep it or if it is unlawful to continue to keep it.

Restriction You can request that the use of your personal information is limited to storage only and that we use it for no other purpose. This applies where you contest the accuracy of the personal information we hold, or our use of the information is unlawful, or we no longer need the information except in relation to legal claims, or you object to the use of your data and we need to verify whether or not our purpose for keeping it overrides the grounds of your objection.

The Information Compliance team can be contacted by email on compliance@lincoln.ac.uk or by post at: Information Compliance, Secretariat, University of Lincoln, Brayford Pool, Lincoln, LN6 7TS.

How to object or withdraw consent

If you object to our use of your personal information, then we must stop unless we can demonstrate compelling legitimate grounds for continuing. Please contact your HR Business Partner in the Human Resources Department and explain the grounds of your objection.

If you have provided your consent for the use of your personal information, then you can withdraw this consent at any time via contacting the Human Resources Department or third party provider as appropriate.

If you object to our use of your personal information in either the Computer-aided Facility Management or the Salto Systems Access software, please contact the Estates Support Desk on 01522 886777 or estatessupport@lincoln.ac.uk and explain your objection.

How to contact us

For general enquiries please call 01522 88 2000 or write to University of Lincoln, Brayford Pool, Lincoln, LN6 7TS.

You can find contact details for individual teams and staff by visiting <http://staff.lincoln.ac.uk>.

If you have a query about your personal information rights then please contact the Information Compliance team by email on compliance@lincoln.ac.uk or by post at Information Compliance, Secretariat, University of Lincoln, Brayford Pool, Lincoln, LN6 7TS.

How to complain

If you feel that we have let you down in relation to your information rights then please contact the Information Compliance team by email on compliance@lincoln.ac.uk or by post at Information Compliance, Secretariat, University of Lincoln, Brayford Pool, Lincoln, LN6 7TS.

You can also make complaints directly to the Information Commissioner's Office (ICO). The ICO is the independent authority upholding information rights for the UK. Their website is ico.org.uk and their telephone helpline number is 0303 123 1113.