

## EMPLOYEE PRIVACY NOTICE

**Data controller:** Lincoln College, Monks Road, Lincoln, LN2 5HQ

**Data Protection Officer:** Cheryl Maxwell (Governance Officer) – [dpo@lincolncollege.ac.uk](mailto:dpo@lincolncollege.ac.uk)

The organisation collects and processes personal data relating to its employees to manage the employment relationship. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

### What information does the organisation collect?

The organisation collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your working pattern schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including performance reviews, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information (all the protected characteristics as detailed in the Equality Act).

The organisation collects this information in a variety of ways, for example through:

- application forms or CVs;
- passports or other identity documents such as a driving licence;
- forms completed by you at the start of or during employment;
- correspondence with you;
- interviews, meetings or other assessments.

The organisation may also collect personal data about you from third parties, such as references supplied by former employers and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your HR file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

## **Why does the organisation process personal data?**

The organisation needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit entitlements.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure compliance with duties in relation to individuals with disabilities, meet obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

The organisation relies on one or more of the following lawful bases under Article 6 UK GDPR when processing employee data: performance of a contract; compliance with a legal obligation; legitimate interests pursued by the organisation; or consent (where this applies).

For special category data, the organisation relies on conditions in Article 9 UK GDPR, including employment, social security and social protection law; occupational health purposes; and substantial public interest (e.g. equality monitoring).

## **Who has access to data?**

Your information will be shared internally, including with members of the People Service team, CIS team, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

The organisation shares your data with third parties in order to obtain pre-employment references from other employers and obtain necessary criminal records checks from the Disclosure and Barring Service. The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation also shares your data with third parties that process data on its behalf in connection with the provision of benefits and the provision of occupational health services.

The organisation may also be required to share your data, i.e. your name and work contact details, with a third party for the following reasons:

- for the provision of training where this is a requirement for you to carry out your role, for example where the training is provided online by an external provider;
- when liaising with other organisations, i.e. awarding bodies.

The organisation will not routinely transfer your data outside the UK. Where data is transferred outside the UK, this will only take place where appropriate safeguards are in place.

## **How does the organisation protect data?**

The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the organisation engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

## **For how long does the organisation keep data?**

The organisation will hold your personal data for the duration of your employment. After your employment ends, data will be retained for different periods depending on the type of record. For example: personnel records are normally retained for 6 years after employment ends; payroll and tax records are retained for 6 years; recruitment records are normally retained for 12 months. Where exact retention periods cannot be specified, the organisation applies criteria based on legal requirements and business needs.

## **Your rights**

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;

- object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing;
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing;
- request the portability of your personal data, allowing you to receive it in a structured, commonly used, machine-readable format and transmit it to another controller, where processing is based on consent or contract and carried out by automated means.

The organisation does not carry out automated decision-making, including profiling, that has a legal or similarly significant effect on employees.

If you would like to exercise any of these rights, please contact the People Services Unit. You can make a subject access request by completing the organisation's form for making a subject access request (see Data Protection Policy).

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner's Office (ICO):

ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF  
Helpline: 0303 123 1113  
Website: [www.ico.org.uk](http://www.ico.org.uk)

### **What if you do not provide personal data?**

You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.