



PRIVACY NOTICE - Employees

1. WHO WE ARE AND HOW TO CONTACT US

- 1.1. We are Leicester College (the “College”). This privacy notice sets out how and why we use personal information, and your related rights.
- 1.2. For the purposes of applicable data protection law (mainly the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018)), we are the “controller” of your personal information. That means that we determine the purposes and the means of using your personal information (ie “why” and “how” your personal information is used), and that we take on legal obligations to you.
- 1.3. If you have any questions or queries which are not answered by this Privacy Notice, or have any potential concerns about how we may use the personal data we hold, please write to the Data Protection Officer at Leicester College, Freeman’s Park Campus, Welford Road, Leicester, LE2 7LW or email dpo@leicestercollege.ac.uk.

2. WHAT INFORMATION DO WE HOLD ABOUT YOU?

Information we collect from you

- 2.1. When you applied to the College you provided us with personal data via the online or paper based application routes. This included your name, address, date of birth, contact information, gender, next of kin, previous education, previous employment and medical information including whether you have a disability. We also collected sensitive information about ethnicity, religion, nationality and sexual orientation.
- 2.2. When you became an employee we collected additional information including your bank account details, medical history and previous attendance at work, references from previous employers and information on background checks and criminal records checks. This may be stored in a paper or electronic personal file or in the HR Database.

Other information

- 2.3. During your employment we also hold other information about you including your attendance, disciplinary, capability or grievance records, staff development, appraisal and performance data, this may be stored in a paper or electronic personal file or in the HR Database.
- 2.4. We may keep information contained in any correspondence by post or email. We may record phone calls. We will also monitor the use of the College’s IT systems in line with the College’s E- Communications Policy, Safeguarding and Prevent Policy and other College policies.
- 2.5. If you leave the College we will provide access to your One Drive files to your immediate line manager.
- 2.6. We may record access to College buildings using the secure key card system. These records are deleted each week and would only be used in the event of an emergency

evacuation.

- 2.7. There may be occasions at College events, when photographs are taken to be used for business purpose including publicity. Notices will be displayed at such events to remind you that this is the case and asking that you let us know if you do not wish your photograph to be included.
- 2.8. We may collect audio and video footage of you through the usage of our Body Worn Camera (BWC) system for the purpose of ensuring the safety of our staff and students, and to enable us to investigate incidents thoroughly.
- 2.9. We may also obtain other information about you permitted by law from other sources. This may include social services, the police or other agencies.

Special Category Personal Data

- 2.10. Some of the information outlined above that we collect about you is regarded as sensitive by data protection law. Known as 'special category personal data', this relates to information about your health, racial or ethnic origin, sex life, sexual orientation, religious beliefs, political opinions, trade union membership or any genetic or biometric data that is used to identify you. This information, and any information about criminal offences / convictions, warrants a higher level of protection under data protection law. We therefore apply additional safeguards and information security measures when using these types of your personal information.

3. WHY DO WE COLLECT THIS INFORMATION?

- 3.1. We collect information in order to enable us to fulfil our legal obligations in relation to your employment contract. For example we need to pay you in accordance with your contract and to administer pension entitlements.
- 3.2. In other cases we may need to process personal data, before, during and after the end of the employment relationship in order to enable us to fulfil our legal obligations in relation to providing further education in line with the Further and Higher Education Act 1992, to comply with the requirements of government funding agencies, and to meet other statutory requirements. For example, to maintain employment records, obtain occupational health advice, arrange staff development activities, provide references on request for current or former employees and to respond to and defend against legal claims.
- 3.3. Where we process other personal data such as information about ethnicity, sexual orientation or belief, this is done for the purposes of equal opportunities monitoring. Data that we use for these purposes is anonymised or will be collected with your express consent, which can be withdrawn at any time. You are free to decide whether or not to provide such data and there are no consequences for failing to do so.
- 3.4. Under Article 6 of the [UK General Data Protection Regulation \(UK GDPR\)](#), we are required to have a "lawful basis" to collect and use personal information. A lawful basis is a reason or justification for use which is accepted and recognised by the UK GDPR. The lawful bases we rely on for processing personal information are:
 - where we have your consent;
 - to perform contractual obligations to you;

- to comply with the College’s legal obligations;
- to perform various tasks which are in the public interest, including educating and safeguarding our staff and pupils;;
- where necessary in an emergency situation; and
- where necessary to achieve the College’s “legitimate interests”. In overview, a legitimate interest is any valid and genuinely-held educational, operational, legal or commercial objective; and
- where necessary to achieve a “recognised legitimate interest”. These include, among others, emergencies, detection, investigation or prevention of crime and safeguarding vulnerable individuals.

3.5. Under Article 9 of the UK GDPR, we are required to have a “condition” to collect and use special category personal information (as defined above). A condition is, essentially, an additional lawful basis. The conditions we rely on to collect and use special category personal information are:

- where we have explicit consent;
- where necessary for exercising and/or enforcing ours or your rights or obligations in the fields of employment and social security;
- where necessary in emergency situations;
- where necessary for the establishment, exercise or defence of legal claims;
- where necessary for reasons of medical diagnosis, administration of preventive medicine, the provision of health or social care treatment;
- for public health reasons;
- for research and statistical purposes; and
- where necessary for reasons of substantial public interest (such as equality of opportunity / treatment, preventing / detecting unlawful acts, exercising a protective function, supporting individuals with a particular medical condition, to provide counselling, advice or support and to safeguard children or individuals at risk).

4. WHO MIGHT WE SHARE YOUR INFORMATION WITH?

4.1. We do not share your information with anyone unless the law and our policies allow us to do so. Some of the most likely instances of where we may share your personal information are listed below.

4.2. Your information may be shared internally, including with members of the HR team, (including recruitment and payroll), your line manager, managers in the area in which you work and IT staff if access to the data is necessary for the performance of their roles.

4.3. Sensitive information such ethnicity, disability, religion, nationality and sexual orientation will only be shared internally within the HR Department. We will keep this information about you confidential.

4.4. We may share your personal information with third parties such as HMRC, in order to comply with our legal duties. We may also share the information in an anonymised format, with national bodies for the purposes of monitoring and research.

4.5. We may share your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third party providers and obtain necessary criminal record checks from the Disclosure and Barring Service. We 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.

- 4.6. We also may share your data with third parties that process data on our behalf, for example in connection with payroll, the provision of benefits and the provision of occupational health services.
- 4.7. We may share your information with our professional advisers such as accountants and solicitors.
- 4.8. We may be asked to share data with other third parties where there is a lawful reason for their request. These may include: the police, social services, legal firms acting on your or the College's behalf, insurance companies acting on your or the College's behalf and other government agencies.

5. TRANSFERRING YOUR PERSONAL DATA TO OTHER COUNTRIES

- 5.1. In most cases we expect your information to stay here in the UK. However, on the few occasions where we do transfer your information outside the UK, we will ensure it is protected and handled in line with data protection law.
- 5.2. If we do transfer your personal data, we generally do not expect to transfer it to territories outside the European Economic Area (EEA). However, in instances where we need to do so (for example, where one of our service providers is based outside of the EEA), we will put in place the necessary additional protections required by Article 46 UK GDPR, or rely on one of the exemptions in Article 49 UK GDPR in order to transfer your data.
- 5.3. If you would like more information about how we protect your personal information if it is transferred outside the UK please email dpo@leicestercollege.ac.uk.

6. HOW DO WE PROTECT YOUR DATA?

- 6.1. We take the security of your data seriously and implement technical (i.e. IT/technological) and organisational (i.e. physical/documentary) measures to ensure that your data is not lost, accidentally destroyed, misused or disclosed inappropriately.
- 6.2. Where we engage third parties to process personal data on our behalf, we do so on the basis of written instructions, ensuring they are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7. HOW LONG DO WE KEEP THIS INFORMATION ABOUT YOU?

- 7.1. We keep information in accordance with our document retention policy. Retention periods are in line with the length of time we need to keep your personal information in order to manage and administer your contract of employment, carry out our statutory functions or public interest tasks, establish or defend legal claims, or ensure the success of any of our legitimate interests. They also take into account our need to meet any legal, statutory and regulatory obligations. These reasons can vary from one piece of information to the next. In all cases our need to use your personal information will be reassessed on a regular basis and information which is no longer required will be

anonymised or deleted.

8. AUTOMATED DECISION-MAKING

- 8.1. Automated decision-making is when a computer or similar electronic system uses personal information to make decisions about people without any human involvement. Profiling involves collecting various pieces of information about a person in order to analyse or evaluate certain aspects relating to that person or to make predictions about them (for example, how that person may behave or what their preferences are). Automated decision-making does not have to involve profiling, though it often will.
- 8.2. We do not use your personal information in automated decision-making, including profiling (i.e. we do not create profiles or make decisions about you based solely on automated decision-making without human involvement). If that changes, we will tell you.

9. WHAT ARE MY RIGHTS?

- 9.1. The UK GDPR gives you certain rights regarding how your information is collected and used. To exercise any of these rights, contact dpo@leicestercollege.ac.uk.
- 9.2. You have the following rights:
- the right to be informed about the collection and use of your personal data – this is called 'right to be informed';
 - the right to ask us for copies of your personal information we have about you – this is called 'right of access', and is also known as the right to make a subject access request (SAR), data subject access request or right of access request;
 - the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification';
 - the right to ask us to delete your personal information – this is called 'right to erasure';
 - the right to ask us to stop using your information – this is called 'right to restriction of processing';
 - the 'right to object to processing' of your information, in certain circumstances;
 - rights in relation to automated decision making and profiling;
 - the right to withdraw consent at any time (where relevant); and
 - the right to [complain to the Information Commissioner](#) if you feel we have not used your information in the right way.
- 9.3. Please note that some of these rights are only available in certain circumstances and may be subject to legal exemptions.
- 9.4. There are legitimate reasons why we may refuse your information rights request. For example:
- the right to erasure does not apply when the use of the data is necessary in order to comply with a legal obligation; to establish or defend a legal claim; or to carry out a task in the public interest;
 - the right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests;
 - right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent.

- 9.5. We may also refuse your request if it is manifestly unfounded or excessive.
- 9.6. If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance. We will acknowledge all complaints within 30 days and aim to deal with them without undue delay..

10. PRIVACY NOTICE CHANGES

- 10.1. This Privacy Notice is regularly reviewed. This is to make sure that we continue to meet the highest standards and to protect your privacy. We reserve the right at all times, to update, modify or amend this Notice. We suggest that you review this Privacy Notice from time to time to ensure you are aware of any changes we may have made. The latest version of this Notice can be found on the College's website.