EMPLOYEE PRIVACY NOTICE

Chesterfield College (and its subsidiary companies) collects and processes personal data relating to its employees to manage the employment relationship. The college is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the college collect?

The college 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 college.
- Information about your remuneration, including entitlement to benefits such as pensions.
- Details of your bank account, payroll records, tax status and national insurance number.
- Pension details including membership of both state and occupational pension schemes (current and previous).
- Information about your marital status, next of kin, dependants and emergency contacts.
- Information about your nationality and entitlement to work in the UK.
- Information derived from monitoring IT acceptable use standards; photo identification and CCTV images.
- The installation and use of technical measures including firewalls and intrusion detection and retention and regular assessment of the technical security of Group systems, Group staff monitor systems and respond to suspicious activity. Alongside these technical measures there are comprehensive and effective policies and processes in place to ensure that users and administrators of Group information are aware of their obligations and responsibilities for the data they have access to.
- Information about your criminal record.
- Details of your 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 sabbaticals, maternity, paternity, adoption leave and the reasons/nature for the leave;
- Details relating to your performance at work eg probation, reviews, PDR, promotions and any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.
- Whistleblowing concerns raised by you, or to which you may be a party or witness.
- Information relating to your training history and development needs.
- Information relating to your health and wellbeing and other special category data to comply with our legal obligation and equal opportunity monitoring including whether or not you have a disability for which the college needs to make reasonable adjustments. We also use it to ensure the health, safety and wellbeing of our employees including the risk assessments and reasonable adjustments for COVID-19.
- Details of trade union membership.
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

The college collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms

completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the college collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from criminal records checks permitted by law.

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

Why does the college process personal data?

The college 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, pension and insurance entitlements).

In some cases, the college 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, to enable employees to take periods of leave to which they are entitled, and to consult with employee representatives if redundancies are proposed or a business transfer is to take place. 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 college has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the college 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.
- Create and maintain staff photo images for identification and security purposes.
- Operate CCTV within the premises in line with our CCTV & Surveillance Policy.
- 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 that it complies with duties in relation to individuals with disabilities, meet its 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 college 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.
- Conduct employee engagement surveys.
- Provide references on request for current or former employees.
- Respond to and defend against legal claims.

- Maintain and promote equality in the workplace.
- Maintain and promote health, safety and wellbeing in the workplace.

Where the college 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.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is processed to allow the college to operate check-off for union subscriptions.

Where the college processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. You can ask us to stop processing this data at any time.

Lawful basis for processing your personal data

Depending on the processing activity, we rely on the following lawful basis for processing your personal data under the GDPR:

• Article 6(1)(b) which relates to processing necessary for the performance of a contract.
• Article 6(1)(c) so we can comply with our legal obligations as your employer.
• Article 6(1)(d) in order to protect your vital interests or those of another person.
• Article 6(1)(e) for the performance of our public task.
• Article 6(1)(f) for the purposes of our legitimate interest.

Special category data

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

• Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
• Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
• Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
• Article 9(2)(f) for the establishment, exercise or defence of legal claims.
• Article 9(2)(j) for archiving purposes in the public interest.

In addition, we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2)(a) and (b) of the DPA 2018. These relate to the processing of special category data for employment purposes, preventative or occupational medicine and the assessment of your working capacity as an employee.

Criminal convictions and offences

We process information about staff criminal convictions and offences. The lawful basis we rely to process this data are:

• Article 6(1)(e) for the performance of our public task. In addition we rely on the processing condition at Schedule 1 part 2 paragraph 6(2)(a).
• Article 6(1)(b) for the performance of a contract. In addition we rely on the processing condition at Schedule 1 part 1 paragraph 1.

Who has access to data?

Your information will be shared internally, including members of the HR and Payroll 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.

Your data may also be shared with employee representatives in the context of collective consultation on a redundancy or business sale. This would be limited to the information needed for the purposes of consultation, such as your name, role and length of service.

All offers of employment are conditional until satisfactory completion of the mandatory pre-employment checks. All pre-employment checks are conducted in line with the government's Keeping Children Safe in Education guidance. The college shares your data with third parties in order to complete our pre-employment checks,which include the Disclosure and Barring Service; references are obtained from other employers, employment background checks from third-party providers and necessary criminal records checks . The college will carry out online searches as part of due diligence on shortlisted candidates. This may help identify incidents or issues that have happened and are publicly available online, any information highlighted will be discussed at interview.

The college 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 college also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services. The college will not transfer your data to countries outside the European Economic Area.

Disclosures under the Freedom of Information Act

As a public authority we receive information requests under the Freedom of Information Act (2000) about our staff and we must consider whether to disclose staff information (including agency and temporary staff) in response to these requests. We will normally disclose work-related information about staff in a public-facing role. We may also disclose information about staff members whose work is purely administrative if their names are routinely sent out externally. It is less likely that information about those who do not deal directly with the public in an operational capacity will be disclosed. We will consider withholding information if we think that it will prejudice our regulatory role or the rights and safety of our staff, irrespective of grade or position.

The type of information you can expect we will disclose is as follows:

- Name and work contact details.
- Pay bands (not your exact salary).
- How long you have worked at Chesterfield College, your current role, any previous roles or secondments and what your role involves.
- Your position in the corporate structure.
- Business related entries in your diary/calendar.
- Summaries of expense claims without details of where you stayed, where you ate or your itinerary.
- Any work related training
- Any work related opinions, for example ILP notes, comments containing your opinion about a student, investigation or a complainant.

The list above does not include every area where we might disclose information about you. The type of information provided will only concern your professional life within the Chesterfield College Group. We will not disclose non-work related personal or special category data.

When asked to disclose diary or calendar information due consideration will be given to the safety of our staff. Where this information is requested outside of an FOI request our staff are advised to consult with their manager before sharing information about a staff member, especially when it concerns movements or whereabouts.

We will consult with you prior to deciding whether to disclose any information that we consider would not be within your reasonable expectations.

Before you begin working with the Chesterfield College Group, contact HR if you need to make us aware of a specific reason why your information cannot be provided as part of a disclosure. At a later point, if you have concerns about information being released you need to inform us of this fact.

How does the college protect data?

The college takes the security of your data seriously. The college 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 college 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 measures to ensure the security of data.

Where do we disclose, share and store data?

We will not sell your personal data.

The Chesterfield College Group is based in the UK and we may store our data within the European Union. Some organisations that provide services to us may transfer personal data outside of the EEA but we will only allow them to do so if the data is adequately protected.

All of the personal data we collect is processed by our staff in the UK. For the purposes of IT hosting and maintenance, this information may be located on servers within the European Union and, occasionally, trusted parties outside the EU may have access to certain parts of the data we collect. No third parties have access to your personal data unless UK or EU law allows them to do so, or an official processing agreement is in place with the Chesterfield College Group.

For how long does the college keep data?

The college will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are up to 13 years, in line with the college's occupational pension regulations.

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 college to change incorrect or incomplete data.
- Require the college 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 college is relying on its legitimate interests as the legal ground for processing.
- Ask the college to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the college's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact the Data Protection Officer at dataprotection@chesterfield.ac.uk. You can make a subject access request by completing the college's Data Subject Request Form, which can be located on the college's staff intranet: https://intranet.chesterfield.ac.uk/DataProtection/

If you believe that the college has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the college 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 college 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, must be provided to enable the college to enter a contract of employment with you. If you do not provide other information, this will hinder the college's ability to administer the rights and obligations arising, as a result of the employment relationship efficiently.