



Privacy Statement

Privacy Statement

Although we haven't changed the way we use your information we would like to remind you of the details of how we use it and who we share it with. The College 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.

We are the data controller of personal information about you. We are: North East Surrey College of Technology (Nescot). Our address is: Reigate Road, Ewell, Surrey, KT17 3DS.

Our Data Protection Officer is Susanne Wicks. If you have any questions about this policy or the ways in which we use your personal information, please contact our Data Protection Officer at dataprotection@nescot.ac.uk, 0208 394 3004.

This privacy notice has been prepared in accordance with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

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 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 work patterns (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, 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 appraisals, performance reviews and ratings, 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 College needs to make reasonable adjustments;
- details of trade union membership; and
- 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 online applications forms; CV's or resumes; obtained from your passport or other identity documents such as your driving licence; from online 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 and information from employment background check providers, information from credit reference agencies, information obtained from social media monitoring and information from criminal records checks permitted by law.

Data is stored in a range of different places, including on your electronic personnel file, in the College's HR and Payroll 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 benefits such as pensions.

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 and 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 also necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question. It may also be necessary to process criminal records data in the context of disciplinary or grievance proceedings for example to investigate and take appropriate action if you are suspected of committing an offence (whether at or outside work).

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;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- ensure employees are complying with relevant policies and procedures
- 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, shared parental leave and parental bereavement 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 and enforce its legal rights; and
- maintain and promote equality in the workplace.

The College relies on legitimate interests as a reason for processing this 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, or racial or ethnic origin, is processed to carry out employment law obligations (such as those in relation to employees with disabilities, for health and safety purposes and the ensure that employees have the right to work in the UK). 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. Data that the College uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time by contacting human resources. Employees are entirely free to decide whether to provide such data and there are no consequences of failing to do so.

As noted above, the College may process criminal records data to assess your suitability for employment both when you are recruited (through appropriate criminal records checks) and in the course of your employment.

Who has access to data?

Your information will be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the area of the College you work in and IT staff if access to data is necessary for the 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 name, contact details, role and length of service.

The College shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third party providers, obtain necessary criminal records checks from the Disclosure and Barring Service, or report suspected offences to the appropriate authorities. The College may also share your data with third parties for the purposes of enforcing its legal rights. The College may 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 specific 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 UK.

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 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. In addition, there are other internal policies and controls such as systems restrictions.

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 and collegial measures to ensure the security of data.

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 set out by relevant retention periods.

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; and
- 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 by email at dataprotection@nescot.ac.uk. You can make a subject access request by contacting the human resources department (humanresources@nescot.ac.uk). 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, have to 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.

Automated decision-making

Employment decisions are not based on automated decision-making

VERSION	1.0
Policy Originator	Human Resources
Approved by:	Assistant Principal HR and OD Director of Personal Development, Behaviour and Welfare
Date Approved:	12 th January 2023
Review Interval:	3 Years
Last Review Date:	12 th January 2023
Next Review Date:	1 st January 2026
Audience:	Staff

