Privacy Notice Workforce (our Staff) – How we use your personal data

Data Controller: Kirklees College, Manchester Road, Huddersfield, HD1 3LD

Data Protection Officer: Carol Tague, GDPR@kirkleescollege.ac.uk

This notice explains how we collect, store and use personal data about our workforce. Our 'workforce' includes anyone working for us, whether on a permanent, temporary, casual or hourly paid basis.

The information we collect and process may include:

Type of data	Examples (not an exhaustive list)
Contact details	full name, address and contact details, including personal and work email address(es) and personal and work telephone number(s)
Personal non-contact details	date of birth, age, sex, marital status, dependents, photographs, video imaging, voice recording, car registration plate, insurance and MOT status, passport details, visa details, driving licence, details of your availability and right to work in the UK, National Insurance number, dietary requirements, hobbies and activities, likes/dislikes/preferences In addition, we process video and still images and sound captured by our ICT network monitoring software
Payroll and other financial information	student loan, bank details, child maintenance, tax/national insurance details, pension, debts to the College, any purchase history
Location	physical or electronic information which identifies your location, including ID card building access data
'Special Categories of Data' (these are recognised as being more sensitive in nature and have a higher level of protection in law)	depending on our relationship with you, the context, and the information you choose to provide, including by using our monitored ICT network, this may include information about your racial or ethnic origin, nationality, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data (e.g. fingerprints used for ID purposes), health, mental health, physiological and disability information, sex life and sexual orientation
Online/Unique identifiers	ID codes, online/website details e.g. usernames, passwords, session IDs, geo locations, device IDs, IP addresses, cookies
Qualifications, training and skills	exam results, qualifications, CPD, professional body memberships, accreditations, certifications
Commitments that may be a conflict of interest	other employment, voluntary positions, elected positions, self-employment
Employment history	previous employers, start/end dates, salary and benefits, references
Employment details	terms and conditions, job title, job description, information about your remuneration, including entitlement to benefits such as pensions or insurance cover, staff ID cards and ID no, teacher ref no, hours worked, start/leave dates, annual leave details, absence/sick leave details/reasons, performance details including appraisals, performance reviews and ratings, improvement plans, disciplinary details and any sanctions taken against you, references
Next of Kin/Emergency Contact	name(s) and contact details
Complaints/Grievances	details from student, staff, public and other complaints to which you are the complainant, a named party or involved in an investigation

Health and Safety information	such as accident records, risk assessments, occupational health records, personal protective equipment records, industrial disease monitoring records; insurance and legal claims, disability and access requirements
Criminal and Conviction Information	any criminal record (or the fact that you have none), Disclosure Barring Service checks and disclosures provided to us and other notifications

Collecting and Storing this information

We collect information in various ways, for example, application forms, CVs or resumes, by email or verbally; from your passport or other identity documents such as your driving licence; from correspondence with you and others; through interviews, meetings or other assessments; in reports; in notes/recordings of meetings; via our electronic databases, forms, Team chat function, email, etc.; medical information provided by occupational health services, your GP, consultant, etc.; any assessments or evaluations carried out by external consultants, information provided in customer compliments, complaints or queries; information from our CCTV cameras; entry and exit data from ID passcards; login details and any other data shared using our college ICT network, including still and moving images; information provided by external bodies such as HMRC, the Child Maintenance Service, and suppliers we contract with for salary sacrifice schemes.

We may collect your personal information from other sources, for example when you provide your details for marketing purposes, register for events, register as a student, or provide us with any other information during your course or apprenticeship. Your personal information may also be provided to us by various third-party sources, which may include previous employers, course providers, HMRC, recruitment agencies, other institutions involved in joint programmes.

Data will be stored securely in a range of places, including in the College's Civica data management system and in other IT systems (including the College email system).

Why does the College process workforce personal data?

Some of the reasons listed below for collecting and using your personal data overlap and there may be several grounds which justify our use of it.

- To enter into and manage contracts:
- To operate our recruitment, selection, and appointment processes;
- To meet our obligations under contracts, for example, to pay salaries, make national insurance contributions, process sick pay, maternity or paternity pay and redundancy pay, reimburse expenses, assess working capacity and make adjustments, and administer leave, benefits, pension and insurance entitlements;
- To keep personnel records up to date and accurate;
- To renegotiate, amend and terminate contracts;
- To manage contracts with employers, funding bodies, subcontractors, etc.;
- For performance management;
- To make and manage agreements with recognised trade unions;
- If we need to transfer your employment to someone else, for example on a merger;
- To provide access to learning, training and development, including to book accommodation and arrange any adjustments/dietary arrangements;
- To operate opt-in salary sacrifice schemes such as Childcare vouchers and Cycle to Work;
- To support transactions with third parties when required, relating to funding for training, e.g. the government apprenticeship service;
- For the purpose of processing payments in return for goods or services (including staff employed via a recruitment agency);
- To pay professional fees and subscriptions to maintain professional memberships.
- To perform a task in the public interest:

- To manage staff in the delivery of teaching and in their research and other academic activity;
- To complete and return Government Data Collection Returns;
- To monitor the size and makeup of the workforce and for succession planning;
- To monitor the completion and currency, as well as the impact, of staff training;
- To record entry and exit to our buildings/campuses;
- To manage our car parks;
- To plan for the safe and efficient movement of people and traffic on and around our campus;
- To take photographs for the purpose of providing Staff ID cards;
- To use CCTV recording and images and monitor our ICT network for safety and security purposes;
- To keep track of our ICT hardware and other equipment;
- To protect our assets and assist in the detection, investigation and prevention of crime.
- To consider and respond to compliments, concerns and complaints;
- To meet our legal obligations:
- To establish and maintain effective corporate governance;
- To record and report delegations and decisions;
- In the handling of staff grievances and disciplinary matters;
- To carry out pre-appointment checks;
- To comply (and monitor compliance) with our statutory duties in respect of e.g. equality, safeguarding, health & safety, data protection, public interest disclosures, etc.;
- To respond to a data breach;
- To monitor incidents, accidents and near misses, to investigate, report as necessary to external agencies and make and respond to claims.
- To protect the vital interests of data subjects:
- To respond to medical emergencies;
- To process next of kin/emergency contacts details.
- For our legitimate interests or those of a third party:
- To provide employment references;
- To enable trade union representatives to contact prospective members and support members;
- To provide feedback to job applicants and agencies;
- To run and promote wellbeing workshops and activities;
- To collect and analyse staff responses to monitoring questions, for example about caring responsibilities, to support our diversity and inclusion agenda;
- For marketing purposes;
- To operate our campus CCTV system, to protect our community and to monitor the flow of vehicles and pedestrians around our campus;
- For some marketing activities and to use images and videos in our marketing materials (including in some circumstances sharing data with other publishers) in order to promote our products and services;
- To share relevant information with the police and other agencies engaged in safeguarding, child protection and the prevention of crime; and
- In some cases, to share information with our legal advisors for legal advice.

Our lawful bases for using this data (Information Commissioner Guidance)

We only collect and use your personal data when the law allows us to. Most commonly, we use it where we need to:

- Carry out a task in the public interest;
- Comply with a legal obligation; or
- Comply with a contractual obligation.

Less commonly, we may use personal information about you where:

- We have (or a third party has) a legitimate interest in processing it;
- You have consented;
- We need to protect your vital interests (or someone else's).

We maintain a record of processing activities which sets out the lawful basis for all our processing activities and, in each case, the purposes of the processing, a description of the categories of individuals and of personal data, the categories of recipients of personal data, details of transfers to third countries, including a record of the transfer mechanism safeguards in place, retention periods and a description of the technical and organisational security measures we have in place to protect the data.

Who has access to your data?

Your information may be shared internally within college where this is necessary or expedient for the performance of staff roles and/or for the delivery of our services, products or programmes, or to comply with any contractual agreement, law or regulation. We do not share your personal data with any third party unless the law allows us to do so.

To enable us to comply with our legal and contractual obligations and to enable the conduct of business, we may need to share your personal information as follows:

Routinely:

- Business system providers/suppliers and service providers in connection with work related activities and systems access, to enable them to provide the service we have contracted for;
- Pension providers and payroll providers;
- HM Revenue and Customs;
- Disclosure and Barring Service – to check for criminal convictions and offences;
- We provide new starter names and start dates to the trade unions so that they can contact employees for potential membership purposes. We may also share your data with the trade unions during formal processes that involve trade union consultation, such as restructures, or where a trade union is representing you. Upon instruction from you or from the Trade Union on your behalf, we will also share information in relation to salary reductions for Trade Union membership fees.
- Previous and future employers/referees – pre and post contract checks and, where relevant, pre-transfer due diligence;
- External Training/Travel Providers – booking and administration purposes;
- Recruitment and employment sites and agencies;
- We outsource the continuous monitoring of all activity on our IT networks and this is done primarily by artificial intelligence which flags any concerns for review by the outsourced data processing team. Relevant data is passed to the College for safeguarding and child protection purposes.
- We use videoconferencing software, predominantly Microsoft Teams but also other platforms, to deliver and manage online meetings, training sessions, conferences, webinars, events and workshops, allowing participants to log in and attend, or in some cases view the content later. Any personal information you submit when you register with Microsoft Teams, Skype etc. will be stored by and accessible to that platform. Please only submit personal information which you are happy to have processed. The privacy policy for Microsoft is: https://privacy.microsoft.com/en-GB/privacystatement.

Infrequently:

- Local Authority/Local Safeguarding Board/Social Care Teams/LADO - for safeguarding purposes;
- Health and Safety Executive – to report accident information/investigation purposes;
- Police and Enforcement Agencies – to assist in the detection, investigation and prevention of crime (this includes the Courts and Coroner Service);
- The Child Maintenance Service in respect of any dependents;
- Emergency services in the event of an emergency;
- In connection with DSAR requests (Data Subject or Authorised Representative);
- Information Commissioner's Office (ICO) (complaints/breaches investigations);
- Awarding/validating bodies for general administration, quality control and queries;
- Courts and Tribunals and Solicitors, Barristers and other legal professionals acting for or against the College (or to unrepresented claimants/respondents) where information is disclosed in connection with a legal claim or application;
- In connection with investigations, disputes, complaints and grievances internally, with third parties such as local authority safeguarding boards, trade unions, government departments and agencies, insurers and legal representatives and professional bodies to which a member of staff is affiliated e.g. CIMA, CIPD.
- Where malpractice is suspected or alleged, with other awarding/validating bodies, the qualifications regulator or other professional bodies - in accordance with relevant policies and procedures.
- Government departments or agencies for government audits, reviews, comply with funding requirements, and data collection requirements e.g. research/analysis/statistics/equality & diversity, benchmarking purposes.
- Childcare/Bike to Work/Dental Plan etc. scheme administrators;
- Mortgage companies/rental agencies.

How does the College protect data?

We have robust internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not inappropriately accessed.

Third Party Processors and Transferring Data Internationally

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

Where we transfer personal data to a country or territory outside the UK and the European Economic Area, we will do so in accordance with data protection law.

For how long does the College keep data?

We will only retain what is necessary in accordance with our Data Retention Policy, which sets out our internal retention and statutory guidelines. Some information must be kept for statutory or contractual reasons for example, Health and Safety records and financial records; this can also apply after your employment ends. Our CCTV camera footage is kept for up to 60 days after which point it will be overwritten unless it is required for some evidential purpose or we have received a data subject access request, in which case it will be retained until the matter has been resolved.

Use of your personal information for marketing purposes

We may send you marketing information by e-mail or text promoting events, campaigns, charitable causes or services that may be of interest to you for up to two years following our last positive contact we have with you. You can "opt out" of receiving such communications by clicking on the "Unsubscribe" link, using the contact details provided, or contacting the Marketing Team or Data Protection Officer.

5 Sept 2023

Your rights

As a data subject, you have a number of rights, which our GDPR Policy explains in detail:

- The right to be informed;
- The right of access and to obtain a copy of your personal data on request;
- The right to require the college to change incorrect or incomplete data;
- The right to require the college to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- The right to object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing.
- The right to data portability; and
- Rights in relation to automated decision making and profiling.

If you would like to exercise any of these rights, please contact GDPR@kirkleescollege.ac.uk. Please note that exemptions may apply when making a request to exercise your rights, for example where we have to retain or process information for legal purposes. For more information on your personal data rights visit www.ico.org.uk/your-data-matters.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your employment with us.

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 must 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 have to provide us with data in compliance with statutory requirements, for example to undergo a DBS check, to evidence your right to work in the UK, or in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to do so 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 us to enter into and maintain the contract of employment. In some cases, if you do not provide information, it will hinder our ability to administer the rights and obligations arising as a result of the employment relationship and it may be impossible for you to start or continue to work for us at all.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

Automated decision-making is done as part of our ICT network monitoring but decisions are always checked by a human operator before any further processing is done.

How to access the personal information we hold about you

Individuals have a right to make a 'Data Subject Access Request' to gain access to personal information that we hold about them. Please refer to our Rights of Individuals Policy for more information on how to make a request, or contact our Data Protection Officer at GDPR@kirkleescollege.ac.uk.

Concerns and Complaints

We take concerns and complaints about our collection and use of personal data very seriously. If you wish to query anything within this privacy notice or think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance. Contact our Data Protection Officer at GDPR@kirkleescollege.ac.uk. Alternatively, or if you are not satisfied by the College response to your concern or complaint, you can contact the Information Commissioner. Information is available at http://ico.org.uk/complaints.

Changes to this privacy notice

We will keep this privacy notice under regular review and will place any updates on our website.

6 Sept 2023