Privacy Notice General (Non Staff or Students) – How we use your personal data

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

Data Protection Officer: Jo Green, GDPR@kirkleescollege.ac.uk

This notice explains how we collect, store and use personal data about individuals who interact with us or work with us in a voluntary capacity, i.e. all individuals who are not members of staff or students, such as governors, consultants, volunteers, parent/carers, next of kin, emergency contacts, service users/customers, contractors, assessors, visitors and members of the public.

Depending on your relationship with us, 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, National Insurance number, dietary requirements, hobbies and activities, likes/dislikes/preferences
Financial information	bank details, credit card details, national insurance number and 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)	information about racial and ethnic origin, religion, politics, trade union membership, genetic and biometric data (e.g. fingerprints used for ID purposes), health, mental health, physiological and disability information, sexual orientation, behavioural characteristics, social identity, cultural background, facial images, philosophical beliefs and economic data
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, skills, experience, training, mandatory and voluntary professional body memberships, accreditations, certifications
References and employment details	name and address of your employer and your employment history, including start and end dates, references, Companies House checks
Commitments that may be a conflict of interest	employment, voluntary/elected positions, self-employment, shareholdings and other information about pecuniary and business interests
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
Attendance and Performance data	Records of attendance at meetings or events. Information obtained from any performance appraisals including self-assessments

Collecting and Storing this information

We collect information in various ways, for example through paper and online 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.; 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 data from our college network.

We may collect your personal information from other sources, for example when you provide your details for marketing purposes or register for events. Your personal information may also be provided to us by various third-party sources, which may include employers, course providers, recruitment agencies, other institutions involved in joint programmes, or staff and students may provide your details as an emergency contact.

Data will be stored securely in a range of places, including the College email system.

Why does the College process personal data?

Collecting and processing personal data enables us to comply with our various legal and contractual obligations and conduct our business activities, for example:

- administration and management of our contractual relationship or membership (pre, during and post-contract/appointment), including the maintenance of accurate and up-to-date records and contact details (including next of kin and emergency contact);
- collection and payment in relation to the contract, expenses, provision of goods;
- administration and delivery of meetings, training, conferences, webinars, events/ workshops;
- qualification/academic checks, such as references, DBS checks, driver checks;
- succession planning for roles, committees, panels, offices;
- compliance with our duties to individuals with disabilities;
- providing a safe and secure environment through compliance with Health & Safety law;
- making appointments, bookings and subscriptions on your behalf;
- providing access to campus buildings and systems where applicable;
- compliance with our responsibilities for safeguarding and the Prevent Agenda;
- taking photographs for the purpose of providing an ID card where applicable;
- following up on enquiries from you, visits to open days, non-attendance of interview/enrolments;
- recording entry and exit to our buildings/campuses;
- use of CCTV recording and photographic images for safety and security purposes;
- to assist in the detection, investigation and prevention of crime;
- compliance with our GDPR Data Subject Access Request and Individual Rights obligations;
- alumni membership and fundraising;
- other fundraising initiatives;
- Government, regulatory/funding body or awarding/validating body data collection returns;
- compliance with the Equality Act 2010, including the Public Sector Equality Duty;
- promotion of events, campaigns, charitable causes or services that may be of interest.

We also process personal data with your consent for example for marketing purposes (which you may withdraw at any time by emailing GDPR@kirkleescollege.ac.uk):

Our lawful bases for using your 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).

Where we ask you for information for which we do not have a contractual or legal basis for processing, we will either tell you the legitimate basis for processing or obtain your consent.

Who has access to your data?

Your information will be shared with college staff where necessary for performance of their roles.

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;
- Previous/current employers/referees – pre and post appointment checks and due diligence;
- External Training/Travel Providers – booking and administration purposes;
- We maintain files and registers about specific groups of people for example governors, consultants, volunteers, parent/carers, next of kin, emergency contacts, service users/customers, contractors, assessors, visitors and members of the public. The information contained in these files is kept secure and is only used for purposes directly relevant to your work with us. In some cases we may be legally required to publish such data but will inform you where this is the case;
- 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;
- Some of our meetings, training sessions, conferences, webinars, events and workshops are recorded. Any recordings will be retained and disposed of in accordance with defined timetables set out in our disposal schedule.

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);
- Emergency services in the event of an emergency;
- In connection with Freedom of Information or Environmental Information Requests or DSAR requests (Data Subject or Authorised Representative);
- Information Commissioner's Office (ICO) (complaints/breaches investigations);
- Internal and external auditors;
- 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;
- 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.

- Depending on your role in the College and/or your relationship with us, we may be required to share your personal information with government departments and agencies for example the Education & Skills Funding Agency, to enable them to contact you directly.

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 reasons for example, Health and Safety records and financial records; this can also apply after your involvement with the College 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

Where you have given us consent to do so, 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. You can "opt out" of receiving these texts and/or e-mails at any time by clicking on the "Unsubscribe" link at the bottom of any such communication, or by contacting the contact details on the subscription form or the Marketing Team or Data Protection Officer.

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 involvement with us.

What if you do not provide personal data?

You may have to provide us with data in compliance with statutory requirements, for example to undergo a DBS check. Failing to do so may mean that you are unable to work with us.

Automated decision-making

Decisions about third parties are not based solely on automated decision-making.

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 website 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.

November 2022