Third Party Privacy Notice (not Staff, Students, Governors or Parents)

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 who are not members of staff or students, governors, or parents, such as consultants, volunteers, next of kin, emergency contacts, service users/customers, contractors, assessors, visitors and members of the public.

We collect and process a range of information. Depending on our relationship with you, the information we process may include (but is not restricted to):

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	such as your date of birth, age, sex. We use CCTV at all our sites and may also take photographs and video, for example if recording an event. In addition, we process video and still images and sound captured by our ICT network monitoring software.
Financial information	if we need to conduct any financial transactions with you, such as your bank details, credit card details, and any purchase history
Lifestyle information	such as dietary requirements if you attend a College event
Location	if we issue you with a College ID pass to access our sites, we will collect electronic information which identifies your location
'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, physiological and disability information, politics, trade union membership, sexual orientation, social identity, cultural background, religious and philosophical beliefs
Online/Unique identifiers	ID codes, online/website details e.g. usernames, passwords, session IDs, geo locations, device IDs, IP addresses, cookies
Academic and professional information	such as professional body memberships, accreditations, certifications
References and employment details	name of your employer, references, Companies House checks
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.

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 details and any other data shared using our college ICT network, including still and moving images.

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.

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 relationships, including the maintenance of accurate and up-to-date records and contact details (including next of kin and emergency contact);
- administration and delivery of meetings, training sessions, conferences, webinars, events and workshops;
- invoicing and payments; provision of goods and services;
- providing a safe and secure environment through compliance with Health & Safety law;
- if you are an assessor, administration e.g. invoices, CVs and CPD for the purposes of external quality assurance in relation to your occupational competence to assess student work;
- providing access to our campus buildings and systems;
- compliance with our safeguarding and child protection duties, including the expectation that we closely monitor all use of our IT networks and act on any concerns;
- taking photographs for the purpose of providing an ID card or badge, where applicable;
- following up on enquiries from you, visits to open days, non-attendance of interviews/ enrolments;
- recording entry and exit to our buildings/campuses and movement around the campus;
- 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;
- 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.

You can opt out of any marketing communications 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:

- You have given us express consent to use it in a certain way;
- We need to protect your vital interests (or someone else's vital interests); or
- We, or another person or organisation, have a legitimate interest in processing it, including:
    - 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;
    - In some cases, to share information with our legal advisors for legal advice; and
    - To collect stakeholder feedback to better understand stakeholder perspectives and how they are impacted by our projects and activities, to gain input when planning projects and initiatives, and to better understand the knowledge, attitudes, perceptions, interests and experiences of our stakeholders so we can better meet their needs and improve our engagement and communication plans.

Where you have provided consent for us to use your personal data, you may withdraw it at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal data about you may overlap, and there may be several grounds which justify our use of your personal data in some cases.

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 will be shared within college where this is necessary or expedient for the performance of staff roles and/or for the delivery of the services, products or programmes you are receiving or have received, 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:

<u>Routinely:</u>

- 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/engagement 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 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);
- 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

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 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.

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, 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 visit or work with us.

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.

Sept 2023