

Data Protection and Data Governance Policy

Document Summary

Date of approval: 01/07/26

Approved by: The Academic Board

Last revision date: 25/08/26

Next revision date: 31/08/27

1. Introduction and Purpose

The City College and The City College of Acupuncture, which are collectively referred to as 'the College' in this document, process a significant amount of personal information to fulfil their functions as Higher Education Institutions. This policy outlines how the College complies with the core principles of the UK General Data Protection Regulation, known as the UK GDPR, and the Data Protection Act 2018.

The primary purpose of this policy is to ensure that the College meets its legal and regulatory requirements under data protection laws. This ensures that personal data and special category data are processed lawfully, fairly, securely and in the best interests of individuals. Furthermore, this policy aims to optimise the use of Information Technology to support training, learning, and teaching while ensuring that IT resources remain adequate, secure, and resilient.

The College is fully committed to protecting the personal data it stores, uses, or transfers. It maintains an environment that takes into account the needs of staff and students, both on and off campus.

2. Scope of the Policy

This policy applies to anyone who has access to personal data as part of their relationship with The City College and The City College of Acupuncture. This includes the following individuals.

- All permanent, fixed-term, and temporary staff.
- Registered students and alumni.
- Contractors, agency workers, and subcontractors.
- Volunteers, interns, and agents engaged with the College, whether they are based in the UK or overseas.

This policy should be read in conjunction with the Acceptable Use of IT Policy of the College, which sets out the acceptable use of IT systems and security controls.

Adherence to this policy is mandatory, and non-compliance could lead to disciplinary action or, in the case of third parties, the termination of contracts.

3. Key Definitions

To ensure a clear and consistent understanding of this policy, the following definitions are applied across the institution.

- **Personal Data** means any information relating to an identified or identifiable natural person, who is known as a data subject. Identifiers include names, identification numbers,

location data, online identifiers, or factors specific to physical, physiological, genetic, mental, economic, cultural, or social identity.

- **Special Category Data** refers to sensitive data requiring extra safeguards, which includes race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, and data concerning the sex life or sexual orientation of a person.
- **Data Controller** means the entity, specifically The City College and The City College of Acupuncture, that determines the purposes and means of processing personal data.
- **Data Processor** means a person or body which processes personal data on behalf of the Data Controller.
- **Data Breach** means a security incident involving the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal information.
- **DPIA** means a Data Protection Impact Assessment, which is a formal process used to identify and minimise the data protection risks of a project.
- **Processing** means any operation performed on personal data, including the collection, recording, storage, adaptation, retrieval, consultation, use, disclosure, or destruction of records.
- **Biometric Data** means data resulting from specific technical processing relating to physical, physiological, or behavioural characteristics allowing unique identification, such as facial images.

4. Data Protection Principles

The College must abide by the core principles detailed in Article 5 of the UK GDPR, which require that personal data must follow specific rules.

1. **Lawfulness, Fairness, and Transparency**, which means data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. **Purpose Limitation**, which requires that data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those intentions.
3. **Data Minimisation**, which ensures that data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
4. **Accuracy**, which requires that records are kept accurate and, where necessary, up to date.
5. **Storage Limitation**, which means data must be kept in a form which permits the identification of data subjects for no longer than is necessary.

6. **Integrity and Confidentiality**, which guarantees that data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss.
7. **Accountability**, which dictates that the Data Controller shall be responsible for, and be able to demonstrate compliance with, all the principles listed above.

5. Lawful Bases for Processing

In order for processing to be lawful, the College must meet at least one of the following lawful bases under the UK GDPR.

- **Consent**, where the data subject has given clear consent for the processing of their personal data for one or more specific purposes.
- **Contract**, where processing is necessary for the performance of a contract, such as managing the student relationship and delivering education.
- **Legal Obligation**, where processing is necessary for compliance with a legal obligation to which the College is subject, including reporting to HESA or the OfS.
- **Vital Interests**, where processing is necessary to protect the life of the data subject or another person during an emergency.
- **Public Interest**, where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, including archiving or statistical tasks.
- **Legitimate Interests**, where processing is necessary for the legitimate interests pursued by the College or a third party, except where overridden by the rights and freedoms of the data subject, which covers campus security, CCTV, or alumni relations.

For sensitive or special category data, additional conditions must be met, including explicit consent, employment or social security obligations, protecting vital interests where the subject is incapable of consent, or reasons of substantial public interest. The College uses this data for statistical reporting and providing appropriate support.

6. Individual Rights of Data Subjects

Under the UK GDPR, data subjects have significant rights in relation to their personal data. These rights include the following options.

- **Right to be Informed**, which means individuals have the right to be provided with information on how and for what purpose their data is processed via Privacy Notices.
- **Right of Access**, which allows individuals to request a copy of the personal data the College holds about them through a Subject Access Request.

- **Right to Rectification**, which ensures that inaccurate data must be corrected without delay.
- **Right to Erasure**, also known as the right to be forgotten, which means data should be deleted where there is no legitimate reason for the College to keep it.
- **Right to Restrict Processing**, which allows individuals to limit how the College processes their data in certain circumstances.
- **Right to Data Portability**, which means individuals can receive their data in a machine-readable format to transfer to another organisation.
- **Right to Object**, which means individuals can object to processing based on legitimate interests or for direct marketing.

The College will respond to all rights requests within one month, though this may be extended for complex cases. These rights are not absolute and may not apply in all circumstances.

7. IT Governance and Digital Education

The College is committed to a digital education strategy that ensures staff and students feel confident using available technology. This includes providing equitable and accessible access for all users, in line with the Equality Act 2010 and WCAG standards.

The College utilises platforms such as SharePoint, Moodle, and Microsoft Teams to facilitate online teaching and learning. Use of these systems must be consistent with the broader Information Security policies of the College. Staff are provided with training to ensure they can deliver high-quality synchronous and asynchronous content.

The College records online lectures to support flexible learning, and these recordings are stored securely on designated platforms. Participants will be informed when a session is being recorded. Recordings are used for educational purposes and processed in accordance with applicable data protection legislation and the College's Privacy Notices. Students who have concerns should speak to their lecturer.

Students have the right to opt out of being recorded and should speak to their lecturer if they have concerns. Lecturers must exercise academic judgment to determine if recording is appropriate for sensitive, controversial, or confidential materials. Because recordings are identifiable personal data, data protection law applies to all participants.

A robust cybersecurity framework is maintained in line with guidance from Jisc and the National Cyber Security Centre. The College employs a Securly Web Appliance to filter access to websites, with categories regularly reviewed in line with the Prevent Duty Policy. An audit trail of user access is maintained, with clear processes for investigating suspicious activity while respecting user

privacy. Personal devices must not be connected to the College's internal network unless expressly authorised by the IT team. Where access is required, personal devices should connect through the College's designated guest wireless network. The IT team reserves the right to disconnect any device that threatens network security, compromises data protection, or breaches College policies.

8. Privacy by Design and Impact Assessments

The College has a duty to consider the impact of its processing activities on individuals through privacy by design and default. A primary tool for this is the Data Protection Impact Assessment, which is known as a DPIA.

A DPIA is a legal requirement under Article 35 of the GDPR where processing is likely to result in a high risk to the rights and freedoms of individuals. They should be carried out at the early stage of a project, preferably at the design stage. A DPIA must be completed before any processing activity likely to result in a high risk to the rights and freedoms of individuals.

DPIAs are conducted by the person introducing the new project or process, and project team members can assist them. The steps include identifying the need for a DPIA, describing the nature, context, scope, and purposes of processing, and consulting with relevant stakeholders. The process also requires assessing necessity and proportionality, identifying and assessing risks to individuals, identifying measures to reduce or eliminate risk, and signing off on outcomes under the review of the DPO.

9. Data Breach Management and Reporting

The College has robust procedures for identifying, investigating, and reporting data breaches involving personal information. Adherence to these protocols is essential for legal and regulatory compliance.

It is the responsibility of all staff to report any data breaches without delay. As soon as a breach is identified, it must be reported to the Data Protection Officer immediately at friaz@citycollege.ac.uk. Reporting incidents is not about apportioning blame but protecting the College and its data subjects.

The DPO is responsible for reviewing and investigating all data breaches, regardless of severity. All breaches are recorded in the Data Breach Incident Folder to enable gap and pattern analysis. During an investigation, the DPO will assess the type and sensitivity of information involved, what happened to the information, current protections like encryption, wider consequences, and mitigating actions such as recovering equipment, shutting down IT systems, or changing passwords.

The Information Commissioner's Office, known as the ICO, must be notified of any breach that is likely to result in a risk to the rights and freedoms of individuals. Notification must occur without undue delay and, where feasible, not later than 72 hours after the College becomes aware of it. If notification is delayed beyond 72 hours, it must be accompanied by written reasons for the delay. When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the College will communicate the breach to the affected data subjects without undue delay in a clear, written format. This notification will include the nature of the breach, DPO contact details, likely consequences, and measures taken to address the incident.

10. Data Retention, Security, and Disposal

The College uses technical measures, such as encryption, data masking, and access restrictions, to ensure only authorised personnel with a relevant purpose have access to information.

Pseudonymisation and anonymisation are used wherever possible, and physical security includes making buildings secure and securing equipment.

The College implements multi-factor authentication and complementary technical controls to safeguard institutional systems, user accounts, and personal data.

Multi-factor authentication is required in the following circumstances:

- Logging in from an unrecognised or new device
- Accessing an account from a new geographical or network location
- Any detection of unusual or suspicious login activity
- Completing a password reset
- Scheduled periodic re-authentication

Personal information is kept only for as long as necessary to fulfil the purposes for which it was collected. The College maintains a detailed Data Retention Schedule. Once retention periods expire, data must be disposed of confidentially through shredding for hard copies or secure deletion for electronic records. Data breach records and notes are retained for 6 years from the date of the incident.

11. Staff Training and Responsibilities

Accountability is built directly into the governance structure of the College. The Data Protection Officer identifies and mitigates risks, acts in an advisory capacity, and manages regulatory reporting.

Staff must undertake mandatory training in areas necessary for their job, including data protection, cybersecurity, and Prevent Duty. Completion of training is a contractual requirement

and is monitored by senior leadership. Completion of mandatory training is required to maintain institutional compliance.

Staff must also adhere to DSE Regulations, and the College undertakes regular analysis of screen equipment to mitigate health and safety risks.

12. Contact Information and Complaints

If you have any questions or concerns about how the College handles personal data, please get in touch with the Data Protection Officer.

- Data Protection Officer, Director of Student Records
- Email, friaz@citycollege.ac.uk

The City College operates under INTER-ED UK LTD, which is registered with the Information Commissioner's Office (ICO) under registration number Z2115272.

Individuals have the right to lodge a complaint with the Information Commissioner's Office if they believe their data has not been handled correctly by the institution.