UK COLLEGE OF IT LTD.

PRIVACY POLICY

Document status	Public Privacy Notice / Policy
Version	2.0
Effective date	11 August 2026
Review cycle	At least annually and whenever there is a material change to processing, services, technology or applicable data-protection requirements
Policy owner	Data Protection / Senior Management
Applies to	Applicants, learners, graduates, tutors, staff, contractors, partners, website visitors and other individuals whose personal data is processed by UK College of IT

1. Introduction and Commitment

UK College of IT Ltd. ("UK College of IT", "the College", "we", "us" or "our") respects the privacy of individuals and is committed to processing personal data lawfully, fairly, securely and transparently.

This Privacy Policy explains how the College collects, uses, stores, shares and protects personal data in connection with its website, enquiries, applications, enrolment, education and training services, online learning environments, assessments, learner support, communications and related administration.

The College aims to provide privacy information in clear and accessible language. The UK Information Commissioner's Office (ICO) states that privacy information should be concise, transparent, intelligible, easily accessible and written in clear language.

2. Data Protection Framework

The College processes personal data primarily under the UK data-protection framework, including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) where relevant, and applicable amendments and secondary legislation.

The UK data-protection framework is subject to continuing legislative and regulatory development. The Data (Use and Access) Act 2025 introduced changes that came into force from 2025 onwards, and the ICO has stated that some existing guidance is under review following those changes.

Where another law or binding regulatory requirement applies to a particular processing activity, the College will comply with that requirement.

3. Who Is the Data Controller?

UK College of IT Ltd. is responsible for determining the purposes and means of processing personal data for the activities covered by this Policy, unless another organisation acts as the controller for a particular processing activity.

Registered office: Suite 3.2 Litchurch Plaza, Litchurch Lane, Derby, DE24 8AA

General contact: info@ukcollegeofit.uk

Privacy / Data Protection contact: info@ukcollegeofit.uk

Data Protection Officer: Zsuzsa Galgóczi

4. What Is Personal Data?

Personal data is information relating to an identified or identifiable living individual.

Depending on the circumstances, this may include a name, email address, telephone number, postal address, date of birth, learner number, application information, assessment records, communications, technical identifiers, IP address, device information, photographs, recordings or information contained in correspondence.

5. Special Category and Other Sensitive Data

Some personal data receives additional legal protection, including information concerning health, disability, racial or ethnic origin, religion or belief, sexual orientation, biometric data used for identification and other special-category information.

Special-category data will only be processed where an appropriate UK GDPR Article 9 condition and any additional legal requirements are satisfied.

Information concerning criminal convictions and offences is subject to additional rules and will only be processed where a lawful basis and applicable legal condition exist.

The College will seek to minimise collection of sensitive information and will not request it merely for convenience.

6. Categories of Individuals

The College may process information relating to:

- prospective learners and applicants;
- current learners;

- graduates and former learners;
- parents, guardians or authorised representatives where relevant;
- tutors, assessors and academic staff;
- employees and prospective employees;
- contractors and consultants;
- partner and awarding-organisation contacts;
- suppliers and service providers;
- website users and visitors; and
- individuals who contact the College or whose information is reasonably required for College activities.

7. Categories of Personal Data We May Collect

Depending on the relationship with the College, information may include:

- identity and contact details;
- application and enrolment information;
- programme, module and learner records;
- qualifications and professional experience;
- assessment submissions, marks and feedback;
- attendance or participation information where applicable;
- learner-support and reasonable-adjustment information;
- communications and correspondence;
- payment, invoicing and transaction information;
- technical and device information;
- website usage and cookie-related information;
- complaints, appeals and conduct records;
- safeguarding information where necessary;
- photographs, recordings or video-conference information where legitimately used; and
- information required for certification, verification, quality assurance or legal compliance.

8. How We Collect Personal Data

The College may collect personal data directly from individuals through:

- website forms;
- enquiry forms;
- email and telephone communications;
- applications and enrolment forms;
- learner platforms;
- assessments and submissions;
- support requests;
- complaints and appeals;
- payments and administrative processes; and
- events or online sessions.

The College may also receive information from authorised representatives, partner organisations, awarding or certification organisations, payment providers, technology providers or other lawful sources.

9. Privacy Information at the Point of Collection

Where personal data is collected directly from an individual, the College will provide relevant privacy information at or before the point of collection where required.

The ICO states that privacy information should generally be provided when personal data is obtained, and where data is obtained from another source, information should normally be provided within a reasonable period and no later than one month, subject to applicable exceptions.

Website publication of this Policy supports transparency but does not by itself remove the need for appropriate just-in-time notices where additional information is required.

10. Purposes of Processing

The College may process personal data for the following purposes:

- responding to enquiries;
- assessing applications;
- administering enrolment;
- delivering education and training;
- providing learner support;
- managing assessments and feedback;
- issuing certificates and academic documentation;
- verifying learner identity or qualifications where necessary;
- communicating with learners and applicants;
- administering payments and refunds;
- operating and securing digital systems;
- handling complaints and appeals;
- maintaining academic integrity;
- safeguarding learners and others;
- quality assurance and programme review;
- meeting contractual, legal and regulatory obligations;
- preventing fraud and misuse;
- managing suppliers and partners;
- improving services and user experience; and
- marketing where permitted by law and in accordance with applicable consent and electronic-communications requirements.

11. Lawful Bases for Processing

Depending on the processing activity, the College may rely on one or more of the following lawful bases:

- performance of a contract or steps taken at the individual's request before entering a contract;
- compliance with a legal obligation;
- legitimate interests, where those interests are not overridden by the individual's rights and interests;
- consent, where consent is the appropriate legal basis; and
- protection of vital interests in limited circumstances.

The lawful basis should be determined for the specific processing activity rather than stated as a generic basis for all processing. The ICO requires organisations to identify an appropriate lawful basis and to consider additional conditions for special-category or criminal-offence data.

12. Legitimate Interests

Where the College relies on legitimate interests, it will consider the purpose, necessity and impact of the processing and whether the individual's rights and interests override those interests.

Where appropriate, the College may document a Legitimate Interests Assessment (LIA).

Examples may include proportionate administration, service improvement, network and information security, fraud prevention and certain professional communications, subject to applicable law.

13. Consent

Where the College relies on consent, consent should be freely given, specific, informed and unambiguous and should be capable of being withdrawn.

Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal.

Consent will not be used where another lawful basis is more appropriate simply to create the appearance of choice.

14. Marketing Communications

The College may communicate information about programmes, events or services where permitted by applicable law.

Electronic direct marketing must comply with PECR and other applicable requirements. Where consent is required, the College will obtain appropriate consent and provide a practical method of withdrawing it.

Marketing preferences should be kept separate from essential programme or administrative communications.

15. Cookies and Similar Technologies

The College may use cookies and similar technologies on its website.

Non-essential cookies or similar technologies will be handled in accordance with the College's separate Cookie Policy and applicable PECR requirements.

Where cookie technologies involve personal data, this Privacy Policy also applies to the associated processing.

16. Analytics and Website Security

The College may process technical information such as IP addresses, browser information, device information, security logs and website interaction data where necessary and lawful.

Security logs may be used to protect systems, detect attacks, investigate incidents and maintain service availability.

Analytics processing will be configured according to the College's Cookie Policy and applicable consent requirements.

17. Online Learning Platforms

Depending on the programme, the College may use online learning platforms such as Google Classroom, video-conferencing systems, document platforms or other learning technologies.

These services may process learner identifiers, account information, submissions, communications, participation information, technical data and other information necessary to provide the service.

Third-party platform providers may act as processors, independent controllers or other recipients depending on the service and contractual structure.

18. Assessment and Academic Records

The College may process assessment submissions, marks, feedback, moderation records, examination information, academic-integrity cases, appeals and certification records.

These records are necessary for academic administration, quality assurance, learner progression, certification and the protection of assessment integrity.

19. Learner Support and Accessibility Data

Where learners request support or reasonable adjustments, the College may process information necessary to identify barriers and provide appropriate support.

Health or disability information may constitute special-category data. Such information will only be processed where an appropriate legal condition applies and will be restricted to those who need it for legitimate support, assessment, safeguarding, quality assurance or legal purposes.

The College aims to collect functional information necessary for support rather than excessive medical detail.

20. Safeguarding

The College may process personal data to identify, prevent or respond to safeguarding concerns.

Where necessary to protect an individual or comply with legal obligations, relevant information may be shared with appropriate personnel, professional advisers, awarding organisations or competent authorities.

Safeguarding information may involve special-category or criminal-offence data and will be handled under the applicable legal conditions.

21. Complaints and Appeals

The College may process information contained in complaints, appeals, investigations and related correspondence.

Such processing may be necessary to administer the learner relationship, protect legal rights, investigate concerns, maintain quality assurance and comply with applicable obligations.

22. Academic Integrity and Misconduct

The College may process information relating to suspected plagiarism, collusion, contract cheating, assessment misconduct, prohibited AI use, fraud or other academic-integrity concerns.

Records will be limited to what is reasonably necessary for investigation, decision-making, quality assurance and any applicable appeal or external review.

23. Payments and Financial Information

The College may process billing details, payment records, invoices, refunds and related transaction information.

Where payment processing is performed by a third-party provider, the provider may process payment information under its own privacy arrangements.

The College will not retain full payment-card information where it is not necessary to do so.

24. Identity and Qualification Verification

The College may verify identity, qualifications, professional experience or other information relevant to admissions, certification, programme requirements or fraud prevention.

Where information is obtained from another organisation, the College will provide appropriate privacy information as required by law.

25. Photography, Video and Recordings

The College may use photographs, recordings or video-conference information where there is a legitimate educational, administrative, security, promotional or event-related purpose.

Where consent is required for a particular use, the College will obtain appropriate consent.

Recording of teaching or support sessions will be communicated through the relevant platform or programme arrangements where applicable.

26. Automated Decision-Making and Profiling

The College does not intend to make solely automated decisions producing legal or similarly significant effects on individuals unless an appropriate lawful basis and safeguards are in place.

If the College introduces such processing, this Policy and any relevant just-in-time privacy information will be updated before the processing begins.

Where automated tools are used for administrative, analytics, security or support purposes, the College will assess whether UK data-protection requirements concerning automated decision-making or profiling apply.

27. Artificial Intelligence

The College may use AI-enabled tools for limited administrative, educational, quality-assurance, cybersecurity or service-improvement purposes where lawful and appropriate.

Personal data should not be entered into public or unapproved AI tools unless the College has assessed the relevant privacy, security and contractual implications.

Where AI processing involves personal data, the College will consider transparency, lawful basis, data minimisation, security, accuracy, retention, processor arrangements and any applicable automated-decision safeguards.

28. Data Minimisation

The College will seek to collect and use only personal data that is adequate, relevant and necessary for the stated purpose.

Staff and service providers should avoid collecting personal information simply because it may be useful in the future.

29. Accuracy

The College aims to keep personal data accurate and up to date where necessary.

Individuals are encouraged to notify the College if their personal information changes or if they identify an error.

30. Data Retention

Personal data will not be retained for longer than necessary for the purpose for which it is processed, subject to legal, contractual, academic, financial, safeguarding and quality-assurance requirements.

Retention periods may differ by record type. The College should maintain a Data Retention Schedule identifying categories, retention periods, responsible owners and disposal arrangements.

Where a specific retention period cannot reasonably be fixed in advance, the College may use documented criteria for determining when information should be reviewed or deleted.

31. Academic and Certification Records

Some learner and certification records may need to be retained for longer periods to verify study, awards, assessment decisions, quality assurance, fraud prevention or contractual obligations.

The College will distinguish permanent or long-term academic records from routine administrative correspondence and will not retain every document indefinitely.

32. Data Deletion and Secure Disposal

When personal data is no longer required, the College will seek to delete, anonymise or securely dispose of it.

Paper records should be securely destroyed. Electronic records should be deleted or rendered inaccessible in accordance with the College's technical and organisational procedures.

33. Data Sharing

The College may share personal data with appropriate recipients where lawful and necessary.

Recipients may include:

- tutors and assessors;
- College staff and management;
- learning-platform and IT providers;
- payment and financial service providers;
- awarding or certification organisations;
- professional or regulatory bodies where applicable;
- partner institutions;
- professional advisers;
- insurers;
- auditors and quality-assurance providers;
- safeguarding or competent authorities; and
- other service providers acting on the College's behalf.

34. Data Processors

Where another organisation processes personal data on the College's behalf, the College will seek appropriate contractual and security arrangements.

Processors should only process personal data in accordance with documented instructions and applicable legal requirements, subject to the relevant contractual relationship.

35. International Data Transfers

Some technology, learning, hosting, communication or service providers may process personal data outside the United Kingdom.

Where a restricted transfer under UK data-protection law occurs, the College will use an appropriate lawful transfer mechanism and safeguards where required.

Privacy information should identify relevant international recipients or categories of recipients and the applicable safeguards where the law requires this. The ICO identifies information about overseas transfers and safeguards as part of appropriate transparency.

36. Security Measures

The College will implement proportionate technical and organisational measures to protect personal data against unauthorised or unlawful processing, loss, destruction, damage or unauthorised disclosure.

Measures may include:

- access controls;
- password and authentication controls;
- role-based access;
- secure systems and connections;
- backups;
- malware and security protection;
- staff awareness and confidentiality requirements;
- supplier security controls;
- incident-management procedures; and
- secure disposal.

37. Data Breaches

A personal-data breach may include accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data.

The College will assess incidents and, where required by law, notify the ICO and/or affected individuals within the applicable statutory timescales.

38. Individual Data Protection Rights

Subject to applicable legal conditions and exemptions, individuals may have rights including:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- rights relating to automated decision-making and profiling where applicable.

The exact availability of a right depends on the lawful basis and circumstances of the processing. The ICO identifies access, rectification, erasure, restriction and other rights within the UK GDPR framework.

39. Right of Access

Individuals may request a copy of their personal data and relevant supplementary information, subject to applicable exemptions.

Requests should be sent to info@ukcollegeofit.uk and should contain sufficient information to allow the College to identify the requester and locate the relevant records.

40. Right to Rectification

Individuals may ask the College to correct inaccurate personal data and, where appropriate, complete incomplete information.

41. Right to Erasure

In certain circumstances, individuals may request deletion of their personal data.

The right is not absolute. The College may need to retain information where it has a legal, contractual, academic, safeguarding or other lawful reason to do so.

42. Right to Restrict Processing

In certain circumstances, individuals may request that processing is restricted while an issue such as accuracy, lawfulness or an objection is considered.

43. Right to Object

Individuals may have the right to object to processing based on legitimate interests or certain other grounds.

The right to object to direct marketing is particularly important and will be respected where applicable.

44. Data Portability

Where the legal requirements for portability are met, individuals may request personal data in a structured, commonly used and machine-readable format or request transmission to another controller where technically feasible.

45. Exercising Rights

Data-protection rights requests should be sent to info@ukcollegeofit.uk or Suite 3.2 Litchurch Plaza, Litchurch Lane, Derby, DE24 8AA.

The College may request appropriate information to verify identity and protect against unauthorised disclosure.

The College will respond within the applicable statutory timeframe, subject to lawful extensions or exemptions.

46. Complaints to the ICO

Individuals are encouraged to contact the College first so that concerns can be investigated and resolved where possible.

Individuals also have the right to complain to the UK Information Commissioner’s Office (ICO).

ICO website: https://ico.org.uk/

ICO helpline / postal contact details should be taken from the ICO's current official contact page rather than hard-coded here, as contact details may change.

47. Children and Young People

UK College of IT programmes are generally intended for adult learners unless a programme states otherwise.

If the College processes personal data of children or young people, it will apply age-appropriate transparency and safeguards where required.

The ICO states that privacy information for children should be presented in a way they can understand.

48. Accessibility of Privacy Information

This Policy should be made available in an accessible format and presented in clear language.

Where a person requires an alternative format or reasonable communication adjustment, the College will consider an appropriate solution in accordance with its Accessibility Statement and Learner Support Policy.

49. Confidentiality

Personal data will be shared internally only with people who need it for legitimate purposes.

Confidentiality obligations do not prevent disclosure where required by law, safeguarding, legal proceedings or another lawful and necessary purpose.

50. Third-Party Websites

The College website may contain links to third-party websites or services.

Once a user leaves the College's website, the third party's own privacy and cookie arrangements may apply. Users should review the relevant provider's privacy information.

51. Changes to this Privacy Policy

The College may update this Policy to reflect changes in law, regulatory guidance, services, suppliers, technology or processing activities.

Material changes should be communicated appropriately before new processing begins where required.

The ICO recommends regular review and updating of privacy information and states that new uses of personal data should be brought to individuals' attention before processing starts.

52. Review and Governance

This Policy will be reviewed at least annually and sooner where significant changes occur.

Privacy governance may include:

- maintaining a Record of Processing Activities (where required);
- maintaining a data-retention schedule;
- reviewing processor agreements;
- reviewing international transfers;
- assessing privacy risks and DPIAs where appropriate;
- maintaining data-breach records;
- monitoring data-subject requests;
- reviewing website cookies and tracking technologies; and
- staff privacy and security training.

53. Contact

Privacy / Data Protection: info@ukcollegeofit.uk

General enquiries: info@ukcollegeofit.uk

Learner Support: info@ukcollegeofit.uk

Complaints: info@ukcollegeofit.uk

Registered office: Suite 3.2 Litchurch Plaza, Litchurch Lane, Derby, DE24 8AA

Appendix A – Data Processing / Privacy Information Matrix

Processing activity	Data subjects	Data categories	Purpose	Lawful basis	Recipients	Retention

Appendix B – Data Subject Rights Request Record

Request reference: _____

Date received: _____

Requester: _____

Type of request: Access / Rectification / Erasure / Restriction / Objection / Portability / Other

Identity verification completed: Yes / No

Systems / records searched: _____

Decision / response: _____

Date responded: _____

Extension used: Yes / No

Reason for restriction or refusal, if applicable: _____

Appendix C – Data Breach Record

Incident reference: _____

Date/time discovered: _____

Date/time occurred (if known): _____

Description: _____

Data affected: _____

Individuals affected / estimated number: _____

Risk assessment: _____

Containment actions: _____

ICO notification required: Yes / No / Under assessment

Individual notification required: Yes / No / Under assessment

Corrective actions: _____

Closure date: _____

Appendix D – Privacy Compliance Checklist

☐ Controller identity and contact details are accurate

☐ Privacy contact / DPO status is accurate

☐ Processing purposes are documented

☐ Lawful basis identified for each material processing activity

☐ Special-category conditions identified where needed

☐ Data categories and data subjects documented

☐ Recipients and processors reviewed

☐ International transfers reviewed

☐ Retention periods / criteria documented

☐ Data-subject rights information published

☐ Cookie Policy linked and consistent

☐ Website forms contain appropriate privacy information

☐ Just-in-time notices used where necessary

☐ Data breach procedure operational

☐ Processor agreements reviewed

☐ Privacy risks / DPIAs considered where appropriate

☐ Privacy information reviewed at least annually

☐ Policy updated following material processing changes

Appendix E – Related Policies

- Cookie Policy
- Accessibility Statement
- Equality, Diversity & Inclusion Policy
- Learner Support Policy
- Complaints Policy
- Assessment & Appeals Policy
- Academic Integrity & Plagiarism Policy
- Safeguarding Policy
- Quality Assurance Policy
- Learner Code of Conduct
- Refund & Cancellation Policy