

Privacy Notice – Students and Apprentices

1. Introduction

This Privacy Notice explains how UCS College Group collects, uses, shares, stores and protects personal information about prospective and current students and apprentices. It also provides relevant information for parents, guardians, carers, emergency contacts and other people whom a student or apprentice has nominated as a permitted contact. In this notice, 'student' includes learners on further education, higher education, full-time, part-time and apprenticeship programmes.

UCS College Group is the data controller for the personal information described in this notice. This means that we decide why and how that information is processed.

2. About UCS College Group

UCS College Group is a group consisting of Bridgwater College, Taunton College, Cannington College and Strode College as well as University Centre Somerset.

Name: UCS College Group

Email address: dpo@ucscollegegroup.ac.uk

Data Protection Officer: Emma Kilner

UCS College Group are the data controller for the purposes of data protection law, and we are registered with the Information Commissions Office (ICO) Registration Number **Z4677243**.

3. Whose information this notice covers

This notice covers personal information about:

- people who enquire about, apply for or enrol on a course or apprenticeship;
- current and former students and apprentices;
- parents, guardians, carers, next of kin, emergency contacts and other nominated contacts; and
- individuals connected with a student's education, welfare, support, placement or apprenticeship, where their details appear in our records.

Where we obtain personal information from someone other than the person concerned, this notice provides the information required about that indirect collection, unless an exception applies.

4. Personal data we collect

We may collect, use, store and share the following categories of personal information where they are relevant and necessary:

- Identity and contact information: name, previous names, title, date of birth, gender, addresses, telephone numbers, email addresses, photograph, identity documents, immigration or visa details and student identification details.

- Education and course information: applications, enrolment, attendance, timetables, programme and module details, student work, assessments, examination information, results, qualifications, certificates, prior learning, progress, destination information and individual learning plan records.
- Apprenticeship, employment and placement information: employer and workplace details, job role, employment history, off-the-job training, reviews, progress, attendance, references, professional memberships, placement information and information needed to administer apprenticeship funding and contractual requirements.
- Financial and funding information: fees, payments, refunds, loans, bursaries, benefits, free school meals, travel assistance, household circumstances, sponsorship, funding eligibility, debts, overdue charges, tax or National Insurance information where required, and bank details where payments are made.
- Welfare, support and safeguarding information: pastoral records, learning support, special educational needs and disabilities, Education, Health and Care Plan information, safeguarding concerns, social care or other agency involvement, risk assessments, complaints, disciplinary or malpractice records and information relevant to fitness or suitability to study, work or reside.
- Health and safety information: health conditions, disabilities, access needs, dietary requirements, accidents, incidents, occupational health information, personal protective equipment records, risk assessments and insurance or legal claims.
- Technical, online and location information: student numbers, Unique Learner Numbers, user names, system and portal records, IP addresses, device identifiers, login and audit records, cookies, website usage, physical or electronic access records and location information generated through the use of College systems, equipment or premises.
- Images and recordings: identity-card photographs, CCTV, photographs, audio or video recordings and, where applicable, recorded teaching or online sessions.
- Criminal offence information: criminal convictions, cautions, allegations, Disclosure and Barring Service information and safeguarding or suitability assessments where these are required for a course, placement, apprenticeship or to protect individuals.

We do not routinely require passwords. College systems may store credentials in protected or encrypted form, but students should never disclose their password to another person.

5. Special category and criminal offence information

Some information requires additional protection under data protection law. This may include information about health, disability, racial or ethnic origin, religious or philosophical beliefs, sexual orientation, trade union membership, genetic or biometric data used for identification, and information about criminal convictions or offences. We only process this information where it is necessary, proportionate and supported by an applicable legal condition and appropriate safeguards.

Depending on the purpose, our relevant conditions may include UK GDPR Article 9(2)(a) (explicit consent), Article 9(2)(b) (employment, social security and social protection), Article 9(2)(g) (substantial public interest), Article 9(2)(h) (health or social care) and Article 9(2)(j) (research and statistics), together with an applicable condition in Schedule 1 to the Data Protection Act 2018.

We process criminal offence information under Article 10 UK GDPR and the Data Protection Act 2018 where authorised by law, including for safeguarding, preventing or detecting

unlawful acts, protecting the public, regulatory requirements, and assessing suitability for particular courses, placements or apprenticeships. We apply access controls, retention controls and other safeguards appropriate to the sensitivity of the information.

6. How we obtain personal information

We collect information directly from you through enquiries, applications, enrolment, forms, surveys, meetings, telephone calls, email, online services, assessments, teaching, support services and your use of College premises, systems and equipment.

We may also receive information from parents, guardians or carers; schools, colleges and universities; local and combined authorities; social care, health services, police, youth offending teams and safeguarding partners; employers, placement providers and apprenticeship providers; UCAS; awarding bodies; the Student Loans Company; the Learning Records Service; funding bodies; careers services; professional bodies; and partner institutions involved in joint or subcontracted provision.

Where providing information is mandatory, we will explain this at the point of collection and, where relevant, the consequences of not providing it. Other information is voluntary.

7. Why we use personal information

We use personal information where it is necessary and proportionate to:

- handle enquiries, applications, admissions, enrolment and identity checks;
- deliver, administer and quality-assure education, training, apprenticeships, placements and student accommodation;
- manage attendance, progress, assessment, examinations, achievement, certification and destinations;
- provide learning support, reasonable adjustments, pastoral support and careers services;
- meet safeguarding, Prevent, health and safety, equality and other legal duties;
- administer fees, funding, loans, bursaries, benefits, sponsorship, travel support and debts;
- communicate with students and, where lawful, nominated contacts, parents, guardians, carers, employers and partner organisations;
- operate secure premises, systems and accounts, including identity cards, building access, CCTV, audit logging and crime prevention;
- investigate complaints, conduct, disciplinary, academic misconduct, malpractice and legal matters;
- conduct research, statistical analysis, equality monitoring, service evaluation and improvement;
- meet audit, inspection, regulatory, funding and statutory reporting requirements; and
- promote College services and events where we have an appropriate lawful basis and provide required choices.

8. Our lawful bases

We rely on one or more lawful bases under Article 6 UK GDPR. The basis used depends on the purpose and circumstances of the processing.

Purpose	Typical Article 6 basis	Examples
Education and student administration	Public task; legal obligation; contract	Admissions, enrolment, teaching, assessment, examinations, support and statutory returns.
Apprenticeships and placements	Contract; public task; legal obligation	Training delivery, employer liaison, progress reviews, placement administration and funding compliance.
Safeguarding, Prevent, health and safety	Legal obligation; public task; vital interests where applicable	Protecting individuals, making referrals, managing risk and responding to emergencies.
Fees, funding and financial support	Legal obligation; public task; contract	Fee collection, bursaries, loans, funding eligibility, audits and debt recovery.
Security, crime prevention and legal matters	Public task; legal obligation; legitimate interests	CCTV, access control, incident investigation, legal claims and regulatory cooperation.
Research, statistics and service improvement	Public task; legal obligation; legitimate interests	Statutory reporting, equality monitoring, evaluation, planning and improvement.
Optional marketing and publicity	Consent or legitimate interests, depending on the activity	Promotional communications, optional photographs and campaigns, with appropriate choices and opt-outs.

Where consent is the basis, you may withdraw it at any time. Withdrawal does not affect processing that took place before consent was withdrawn. We will explain any practical consequences, such as whether previously published material can reasonably be withdrawn.

9. Communications with students and contacts

Our principal channel for formal student communications is the College email account and, where applicable, the student portal. Students and apprentices should check these accounts regularly and keep their contact details up to date.

We may use personal email addresses, telephone numbers or text messages where necessary for admissions, enrolment, course administration, attendance, examinations, safeguarding, emergencies, support, payments, debt recovery or other legitimate College purposes. Marketing messages will include an appropriate way to opt out where required.

Students should not automatically forward College email to a personal account because this may weaken security and record-management controls. Unnecessary records should be deleted in accordance with College policies, but students must not delete information that is subject to a legal hold, investigation, complaint, access request or other instruction to retain it.

10. Parents, carers, guardians and nominated contacts

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

We only share personal information where there is a lawful basis and the disclosure is necessary and proportionate. Consent is not the basis for every disclosure.

For students aged 18 or over, we will normally only discuss personal information with a parent, carer, guardian, family member or representative where the student has authorised this, another lawful basis applies, or disclosure is necessary for safeguarding, vital interests, legal obligations or another compelling lawful reason.

For students under 18, we may share relevant information with a person who has parental responsibility, taking account of the student's age and understanding, the nature of the information, safeguarding considerations and any reason why disclosure may not be appropriate. Information may include attendance, behaviour, progress, support and wellbeing where sharing is lawful and necessary.

We will not normally discuss a prospective student's application with another person unless the applicant has authorised this, the applicant is below compulsory school age or another lawful basis or formal information-sharing arrangement applies.

11. Who we share information with

Where lawful and necessary, we may share relevant information with:

- parents, guardians, carers, emergency contacts, representatives and other people nominated by the student;
- employers, sponsors, placement providers, apprenticeship providers and subcontracted education or training providers;
- schools, colleges, universities, partner institutions, careers services, educators, professional bodies, awarding organisations, examining bodies and validating bodies;
- local and combined authorities, virtual schools, social care, health services, safeguarding partnerships, the Local Authority Designated Officer, police, courts, coroners, emergency services and youth offending services;
- the Department for Education, relevant education and skills funding bodies, the Learning Records Service, Ofsted, the Office for Students, Jisc/HESA, UCAS, the Student Loans Company, the Office for National Statistics, the Department for Work and Pensions and other government, regulatory or statutory bodies;
- the Disclosure and Barring Service where a check is required;
- the Health and Safety Executive and insurers where relevant;
- Student Union services where needed to administer membership or services;
- auditors, inspectors, legal advisers and other professional advisers;
- technology, payment, communications, storage, travel, accommodation and other suppliers acting under contract; and
- other third parties at the student's request or where disclosure is required or permitted by law.

We share only the information reasonably required for the relevant purpose. Service providers acting as processors must handle information under our instructions, subject to contractual, confidentiality and security requirements.

For data submitted through education funding and statutory returns, the relevant government or sector body may issue its own privacy notice explaining its further use of the information. Current links should be maintained on the published web version of this notice.

12. Data subject access requests and disclosures

This includes deleted and archived personal information which is still accessible.

When responding to a data subject access request or another rights request, we will carry out proportionate searches of relevant live and archived systems. We may disclose personal information contained in emails, documents, systems, recordings and paper or electronic files where required by law, subject to applicable exemptions and the rights of other people.

13. International transfers

Some suppliers or partner organisations may process personal information outside the United Kingdom. Where information is transferred internationally, we will use a lawful transfer mechanism where required, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, or another approved safeguard. We will also assess and manage relevant transfer risks.

14. Automated decision-making and learning analytics

UCS College Group does not currently make decisions about students based solely on automated processing where the decision produces legal effects or similarly significant effects. If this changes, we will provide specific information about the logic involved, the significance and likely consequences, and the rights available.

We may use attendance, engagement, achievement and support information to identify students who may benefit from contact or support. Decisions and interventions are made or reviewed by authorised staff rather than being determined solely by an automated system.

15. How we protect personal information

We use proportionate organisational and technical measures to protect personal information against accidental or unlawful loss, alteration, disclosure or access. These include role-based access, account security, staff training, policies, contractual controls, secure disposal, incident management, audit logging and additional controls for sensitive information.

Access is limited to staff and authorised partners who need the information for their work. They are required to handle it confidentially and in accordance with applicable policies and instructions.

16. How long we keep personal information

When your course or apprenticeship has ended, we will retain and dispose of your personal information in accordance with our Data Retention and Disposal Policy.

We keep personal information only for as long as it is needed for the purpose for which it was collected and to meet legal, funding, regulatory, safeguarding, audit, insurance and contractual requirements. Retention periods vary by record type.

Examples of records subject to defined retention periods include applications and enrolment records; learning, assessment and examination records; apprenticeship and funding evidence; financial records; safeguarding and support records; health and safety records; complaints and disciplinary records; CCTV; system audit records; and student communications.

The applicable periods and disposal arrangements are set out in the UCS College Group Data Retention and Disposal Policy and retention schedule. Records subject to an investigation,

complaint, legal claim, audit, data subject request or preservation instruction may be kept for longer until the matter is concluded. When information is no longer required, it is securely deleted, anonymised or destroyed.

17. Keeping your information accurate

Please tell us promptly if your personal information changes. Contact the relevant Registry or Student Services team for routine record changes, or email dpo@ucscollegegroup.ac.uk for data protection queries. We may ask for evidence where needed to protect the accuracy and security of the record.

18. Your data protection rights

Depending on the circumstances and the lawful basis, you may have the right to:

- be informed about how your information is used;
- request access to your personal information;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information;
- ask us to restrict processing;
- object to processing, including direct marketing;
- receive information you provided in a portable format where the right applies;
- withdraw consent where processing is based on consent; and
- seek human intervention and challenge a qualifying solely automated decision.

These rights are not absolute. An exemption or limitation may apply, for example where information must be retained or used to meet a legal obligation, protect another person, preserve legal privilege or maintain the integrity of an examination process. We will explain our decision when we respond.

19. Accessing your information or exercising a right

To make a data subject access request or exercise another data protection right, email dpo@ucscollegegroup.ac.uk. Please describe what you are asking for and provide enough information for us to identify the relevant records. We may request proof of identity where this is necessary and proportionate.

20. Marketing

When you have given us consent to do so, we may send your marketing information your personal email and/or college email account promoting events, campaigns and services that may be of interest to you. You can 'opt out' of receiving these messages at any time by clicking the 'unsubscribe' link at the bottom of such communication.

Where permitted, we may send information about events, campaigns, courses and services that may be of interest. We will rely on consent where required and may rely on legitimate interests for limited communications where the law permits. You can opt out of direct marketing at any time by using the unsubscribe link in the message or contacting us. Opting out of marketing will not stop essential communications about your application, course, apprenticeship, safety, support, fees or College services.

21. Concerns and complaints

If you have a concern about how we have handled personal information, please contact the Data Protection Officer at dpo@ucscollegegroup.ac.uk so that we can investigate and respond.

You also have the right to complain to the Information Commissioner's Office. Information about making a complaint is available at <https://ico.org.uk/make-a-complaint/> and the ICO helpline is 0303 123 1113.

22. Changes to this notice

We may update this notice to reflect changes in law, guidance, systems, services or the way we use personal information. The current version will be published on the UCS College Group website. Where a change is significant, we will take reasonable steps to bring it to the attention of affected individuals.