

1. About this notice

This privacy notice explains how Acquire Learning College Ltd collects and uses personal information about people who work for, provide services to or seek work with the College. It also explains the rights you have in relation to your personal information.

We provide this notice because we are responsible for deciding how and why your personal information is used. In data protection law, this means that we are the data controller.

This notice should be read alongside any shorter privacy information provided when you apply for a role, use a particular workforce service or participate in an activity involving an additional use of personal information.

2. Who we are and how to contact us

The data controller is Acquire Learning College Ltd, a company registered in England and Wales under company number 10181287. Our address is Atlas House, Attercliffe Road, Sheffield, S4 7WZ. Information Commissioner's Office (ICO) registration number: ZB915955

Contact	Details
Data protection enquiries	dataprotection@acquirelearning.co.uk
General enquiries	info@acquirelearning.co.uk
Postal address	Atlas House, Attercliffe Road, Sheffield, S4 7WZ

3. Who this notice applies to

This notice applies to:

- job applicants and prospective workers;
- current and former employees;
- workers, agency workers and casual workers;
- contractors, consultants and self-employed individuals;
- visiting tutors, guest lecturers, external assessors and other people engaged to provide services;
- governors and office holders where the College processes their information as part of its workforce administration; and
- emergency contacts, referees, dependants, beneficiaries and other individuals whose information is provided in connection with a member of the workforce.

The Applicant and Student Privacy Notice explains how we use information about applicants and students. The Website and General Enquiries Privacy Notice covers other visitors and enquirers.

4. The information we may collect

The information we collect depends on your relationship with us and the work you undertake. It may include:

Category	Examples
Identity and contact information	Name, title, date of birth, photograph, addresses, email addresses, telephone numbers and emergency contacts.
Recruitment information	Application form, CV, employment history, qualifications, references, interview notes, assessment results, salary expectations and recruitment decisions.
Right-to-work and identity information	Passport or identity documents, nationality, immigration status, visa information and evidence of the right to work in the UK.
Employment and engagement information	Contract, role, department, working pattern, start and end dates, probation, professional registration, duties and changes to employment or engagement.
Pay, tax, pension and benefits	Salary, fees, bank details, National Insurance number, tax information, pension membership, expenses, benefits and deductions.
Attendance and leave	Working hours, attendance, annual leave, family leave, sickness absence and other authorised or unauthorised absence.
Performance and development	Objectives, appraisals, supervision, training, continuing professional development, capability and performance-management records.
Conduct and employment relations	Grievances, disciplinary matters, complaints, whistleblowing, investigations, suspension, conflicts of interest and outcomes.
Health, safety and support	Health or disability information, reasonable adjustments, occupational-health information where used, accidents, risk assessments and support arrangements.
Safeguarding and suitability	Safeguarding concerns, Prevent-related information, declarations, references, criminal-record or DBS information where required, risk assessments and referrals.
Equality information	Age, sex, ethnicity, disability, religion or belief, sexual orientation and other equality-monitoring information where collected.
Technical and monitoring information	College account identifiers, system and network logs, email and communications metadata, device records, building-access information and CCTV where applicable.
Images, recordings and communications	ID photographs, staff profiles, recordings of teaching or events, correspondence and promotional images where applicable.
Leaving and post-employment information	Notice, reason for leaving, exit information, final payments, references, continuing duties and pension or benefit administration.

5. Special category and criminal offence information

Some personal information needs additional protection under data protection law. This includes information about health or disability, racial or ethnic origin, religious or philosophical beliefs, sexual orientation, trade union membership, genetic or biometric identification information, and information about sex life.

We may process relevant special category information to meet employment and equality obligations, provide reasonable adjustments and support, administer absence and benefits, protect health and safety, monitor equality, and respond to safeguarding, welfare or legal concerns. We will only do this where both an Article 6 lawful basis and an additional condition under Article 9 UK GDPR apply.

Where a role, safeguarding responsibility, contractual requirement or law makes it necessary, we may process criminal allegation, conviction or offence information or undertake an appropriate criminal-record check. We will do so only where authorised by law and with the safeguards required by the Data Protection Act 2018.

6. Where we obtain information

We normally obtain information directly from you. We may also receive information from:

- recruitment agencies, employment businesses or online recruitment services, where used;
- referees and former employers;
- educational institutions, awarding organisations and professional bodies;
- government departments, public authorities and immigration bodies;
- the Disclosure and Barring Service and safeguarding bodies, where applicable;
- pension, payroll, benefits, insurance and occupational-health providers, where used;
- students, colleagues, complainants, witnesses and other people involved in College matters;
- emergency services, health professionals, safeguarding partners or law-enforcement organisations where lawful and necessary; and
- College systems and service providers when you use College accounts, networks, devices or premises.

7. Why we use your information and our lawful bases

We must have a lawful basis for each use of personal information. Our principal activities and lawful bases are set out below.

Processing activity	Main Article 6 lawful basis	Additional Article 9 or DPA 2018 condition where relevant
Recruitment, selection, interviews and offers	Steps at your request before entering a contract; legitimate interests in proportionate recruitment administration; legal obligation where applicable	Employment, social security and social protection; equality of opportunity or treatment; explicit consent only where genuinely optional
Identity, right-to-work and pre-employment checks	Legal obligation; steps before contract; legitimate interests where an appropriate suitability check is not legally required	Employment and social protection; substantial public interest conditions; criminal-offence processing only where authorised by law
Managing employment, work or service contracts	Performance of contract; legal obligation	Employment, social security and social protection where special category information is necessary
Payroll, tax, pension, expenses and benefits	Performance of contract; legal obligation	Employment, social security and social protection where relevant
Attendance, leave, sickness absence and family leave	Performance of contract; legal obligation; legitimate interests in workforce planning	Employment, social security and social protection; occupational health where applicable; legal claims
Reasonable adjustments, health support and occupational health	Legal obligation; performance of contract; legitimate interests in supporting staff and safe working where appropriate	Employment, social security and social protection; occupational health; vital interests in an emergency
Performance, appraisal, training, capability and workforce planning	Performance of contract; legitimate interests in effective management, development and service delivery; legal obligation where applicable	Employment and social protection where relevant
Grievances, disciplinary matters, complaints, whistleblowing and investigations	Performance of contract; legal obligation; legitimate interests in investigating and resolving concerns fairly	Employment and social protection; substantial public interest where applicable; legal claims
Safeguarding, Prevent, suitability and risk assessment	Legal obligation; vital interests; legitimate interests in protecting students, staff and others	Substantial public interest, including safeguarding children and individuals at risk; employment and social protection; vital interests; criminal-offence processing where authorised
Equality monitoring and institutional analysis	Legal obligation where applicable; legitimate interests in evaluating equality and workforce effectiveness using appropriately controlled information	Substantial public interest, including equality of opportunity or treatment
Protecting systems, premises, people and information	Legal obligation; legitimate interests in security, business continuity, preventing misuse and investigating incidents	Substantial public interest, legal claims or vital interests where applicable
References, regulatory checks and post-employment administration	Legal obligation; legitimate interests; performance of contract where relevant	Employment and social protection; legal claims where relevant
Optional publicity and non-	Consent, or legitimate interests where	Explicit consent where special category information

Processing activity	Main Article 6 lawful basis	Additional Article 9 or DPA 2018 condition where relevant
essential communications	permitted and appropriately assessed	is intentionally published

Consent will not be used where you have no genuine choice or where the College needs the information to perform a contract, comply with the law or carry out its responsibilities. Where we rely on consent, you may withdraw it at any time without affecting processing already undertaken.

8. Who we may share information with

We share personal information only where there is a proper purpose and lawful basis. Depending on your role and circumstances, recipients may include:

- recruitment agencies, referees and former employers;
- HM Revenue and Customs and other government departments or public authorities;
- payroll, pension, benefits, insurance and expense providers;
- the Disclosure and Barring Service, safeguarding partners and professional or regulatory bodies, where applicable;
- UK Visas and Immigration, where applicable;
- occupational-health, medical, counselling or employee-assistance providers, where used;
- external investigators, mediators, trainers, advisers or employment-law specialists;
- auditors, insurers, legal representatives and professional advisers;
- banks and payment providers;
- IT, cloud, communications, HR, payroll, learning-platform, records-management and other service providers acting for the College;
- students, clients, contractors and partner organisations where limited information is needed for you to perform your role;
- local authorities, emergency services and law-enforcement organisations where necessary and lawful; and
- another organisation involved in a merger, restructuring or transfer of College activities, subject to appropriate safeguards.

We may provide a factual employment reference or other information to a prospective employer, agency, lender, landlord or similar organisation where you have requested or authorised this, or where another lawful basis applies.

9. International transfers

Some of our suppliers or service providers may store or access personal information outside the United Kingdom.

Where a restricted transfer occurs, the College will use a lawful transfer mechanism, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or another mechanism permitted by data protection law. We will also consider whether additional technical or organisational safeguards are required.

You may contact us for further information about the safeguard used for a relevant transfer.

10. How we protect your information

We use technical and organisational measures designed to protect personal information against loss, misuse, alteration, unauthorised access and disclosure. These measures include access controls, confidentiality requirements, staff training, secure systems, backup and recovery arrangements, supplier controls, incident-management procedures and secure disposal arrangements, as appropriate to the information and risk.

Access is limited to people who need the information for an authorised purpose. Staff and service providers are required to protect confidentiality and comply with applicable data protection requirements.

11. Monitoring of systems and premises

The College may monitor appropriate use, security and operation of its systems, networks, accounts, devices and premises. This may include system and access logs, cybersecurity monitoring, email or communications metadata, building-access information and CCTV where applicable.

Monitoring will be proportionate, related to a defined purpose and undertaken in accordance with applicable law and College policies. It is not intended to provide routine intrusive monitoring of private activity. Where more detailed monitoring is introduced, the College will provide appropriate information to affected individuals.

12. How long we keep information

We keep personal information only for as long as it is needed for employment, contractual, legal, tax, pension, safeguarding, health and safety, regulatory, dispute-management and accountability purposes.

Core employment and engagement records may be retained for a period after employment or engagement ends so that we can administer continuing obligations, respond to reference requests and establish or defend legal claims. Payroll, tax and pension records are retained for the applicable statutory or administrative period. Recruitment information about unsuccessful applicants, temporary working records and sensitive supporting evidence are retained only for as long as necessary for their purpose.

Safeguarding, DBS, health, grievance, disciplinary, whistleblowing and investigation records are subject to record-specific retention periods reflecting their sensitivity and purpose. Further information will be provided in the College's Records Retention Schedule.

We may retain information for longer where required for a legal claim, investigation, safeguarding matter, regulatory requirement or preservation obligation. Where possible, information retained for statistical or research purposes will be anonymised.

13. If you do not provide information

Some information is required so that we can consider an application, enter into or perform a contract, pay you, provide workplace benefits, meet legal responsibilities or protect safety. If required information is not

provided, we may be unable to progress an application, enter into or continue an employment or service relationship, make a payment, provide a benefit or meet a requested support need.

Where providing information is optional, we will explain this and any consequences of choosing not to provide it.

14. Automated decision-making

The College does not currently make decisions about applicants or members of its workforce solely by automated means where those decisions have legal or similarly significant effects.

If the College introduces qualifying solely automated decision-making in the future, we will update this notice to explain the logic involved, the significance and likely consequences, and the rights and safeguards available.

15. Your rights

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

- be informed about how your personal information is used;
- obtain access to your personal information;
- have inaccurate information corrected and incomplete information completed;
- have information erased in certain circumstances;
- restrict the use of information in certain circumstances;
- object to certain processing, including direct marketing;
- receive certain information in a portable format;
- withdraw consent where consent is the lawful basis; and
- ask for human intervention and challenge a qualifying solely automated decision.

These rights are not absolute and exemptions may apply. We may need to confirm your identity before responding. We normally respond within one month, although the law permits an extension for complex or numerous requests. We will explain any extension or lawful refusal.

16. Questions, requests and complaints

To ask a question, exercise a data protection right or raise a concern, email dataprotection@acquirelearning.co.uk or write to Acquire Learning College, Atlas House, Attercliffe Road, Sheffield, S4 7WZ.

You also have the right to complain to the Information Commissioner's Office. Information about making a complaint is available at ico.org.uk/make-a-complaint. We would welcome the opportunity to consider your concern first, but you are not required to contact us before approaching the ICO.

17. Changes to this notice

We will review this notice regularly and update it when our activities, systems, suppliers or legal obligations change. The current version will be published on the College website. Where a change could significantly affect you, we will take reasonable steps to bring it to your attention.