Ulearn Education Limited
Privacy Policy

Field	Current entry
Controller	Ulearn Education Limited
Company number	09311556
Registered office	The Elsie Whiteley Innovation Centre, Hopwood Lane, Halifax, HX1 5ER
Website	https://ulearn.education
Main privacy contact	admin@ulearn.education
Admissions contact	admissions@ulearn.education
Privacy Lead / Data Protection Officer	Mr Waseem Ahmed - admin@ulearn.education
ICO registration number	ZA503011
Approver	Musarrat Waseem
Last reviewed	29 April 2026
Version	2.0
Review cycle	At least annually and whenever processing, suppliers, lawful bases, ICO guidance or legislation materially change.
Next scheduled review	April 2027

Privacy Policy

1. Purpose and scope

This Privacy Policy explains how Ulearn Education Limited collects, uses, stores, shares and protects personal information. It applies to prospective students, applicants, learners, website and app users, marketing subscribers, recruitment candidates, employees, workers, contractors, suppliers, university and college partners, agents, event attendees, survey participants and other people who interact with Ulearn.

2. Who we are and who is responsible for personal information

Ulearn Education Limited is registered in England and Wales under company number 09311556. Its registered address is The Elsie Whiteley Innovation Centre, Hopwood Lane, Halifax, HX1 5ER. Ulearn is the data controller for the processing described in this document unless it states otherwise. This means Ulearn decides why and how personal information is used. Privacy matters should be sent to admin@ulearn.education or to the Privacy Lead / Data Protection Contact/ DPO, Mr Waseem Ahmed, at the registered address.

3. Core privacy principles

Ulearn will handle personal information in line with the UK GDPR principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Ulearn will maintain appropriate records, policies, training, supplier controls and evidence to demonstrate compliance.

4. Minimum age for direct use and under-18 data

Ulearn's services are intended for direct use by individuals aged 18 or over. Individuals under 18 should not create an account, submit an online form, upload documents or send personal information directly unless Ulearn has clearly agreed a specific process involving a parent, legal guardian, school, college, university, safeguarding lead or other appropriate adult. Where under-18s are likely to access any Ulearn online service, Ulearn will assess the ICO Children's code/ Age Appropriate Design Code, age assurance, transparency for children and parents, data minimisation, privacy-by-default settings, profiling restrictions, marketing restrictions and whether a DPIA is required.

5. Legal roles

Ulearn may act as controller, joint controller or processor depending on the activity. When Ulearn sends an application, document or enquiry to a university, college, school, training provider, recruiter or employer at an individual's request, that organisation will normally become an independent controller for its own admissions, enrolment, recruitment, immigration sponsorship, student-record or employment processing. Ulearn will document processor and joint-controller arrangements in writing where they apply.

6. Governance and accountability

The Privacy Lead is responsible for coordinating privacy compliance, maintaining this document, records of processing, DPIA logs, supplier due diligence, rights request handling, breach

escalation, training records and review cycles. Senior management is responsible for approving this document, ensuring adequate resources, and embedding data protection by design and default.

7. Personal information Ulearn collects

Category	Examples
Identity and contact details	Name, address, email, telephone number, date of birth, nationality, country of residence, account identifiers and similar contact details.
Education and application information	Course interests, preferred campus/location, qualifications, transcripts, certificates, personal statements, CVs, employment history, academic history, references, English-language evidence, portfolio information and application outcomes.
Admissions and visa-related information	Passport details, proof of funding, visa/immigration information, right-to-study information, CAS-related information, travel or residency details, where applicable and lawful.
Support and safeguarding information	Disability, accessibility, health, wellbeing, safeguarding or support information that is provided or necessary for a specific service.
Recruitment and candidate information	CV, employment history, qualifications, interview notes, right-to-work evidence, references, background checks, equality monitoring where lawful, and recruitment correspondence.
Employee, worker and contractor information	Employment contract details, job title, work contact details, payroll, tax, pension, attendance, leave, sickness, performance, training, disciplinary, grievance, health and safety, emergency contact and benefits information.
Website/app and technical information	IP address, device identifiers, browser type, cookie identifiers, approximate location, log data, pages visited, forms submitted, preferences and security events.
Communications information	Emails, WhatsApp or chat messages, call notes, call recordings where used, enquiry records, feedback, complaints, survey responses and support requests.
Marketing information	Marketing preferences, consent records, opt-in/opt-out status, engagement with emails, events or campaigns, and suppression-list records.
Supplier/partner information	Business contact details, role, organisation, contract details, invoices, bank/payment details where required, due diligence information and business correspondence.
Publicly available or third-party information	Information from education institutions, recruiters, agents, referees, employers, verification providers, public professional sources or other lawful and relevant sources.

8. Mandatory and optional information

Information	Mandatory or optional	Consequence if not provided
Basic enquiry and contact information	Usually mandatory where an individual wants a response or service.	Ulearn may be unable to respond, verify identity, contact

		the person or progress the enquiry.
Course-search and application information	Mandatory where needed for matching, eligibility, admissions support or referral.	Ulearn may be unable to assess options, recommend courses, submit an application or support admissions.
Documents such as passport, certificates, transcripts, CV, English-language evidence and proof of funding	Mandatory only where the relevant institution, immigration process, admissions process or service requires them.	The application may be delayed, incomplete or rejected.
Disability, health, accessibility or support information	Usually optional unless needed for a legal, safeguarding, placement, professional-suitability or employment purpose.	Ulearn or a partner may be unable to arrange reasonable adjustments, support or safeguarding measures.
Equality, diversity and monitoring information	Usually optional unless a legal or regulatory requirement applies.	Choosing not to provide it normally does not affect the application or service.
Marketing consent and preferences	Optional.	The person will not receive optional marketing if they do not opt in or if they opt out. Necessary service messages may still be sent.
Cookies and analytics preferences	Essential cookies are required. Non-essential cookies and similar technologies are optional where consent is required.	Refusing non-essential cookies will not prevent use of core services.
Recruitment, employee and worker checks	Mandatory where required for role, contract, legal compliance, payroll, right-to-work, health and safety or safeguarding.	Ulearn may be unable to progress an application, employ or engage the person, pay them or meet legal duties.
Supplier due diligence and payment information	Mandatory where needed for contract, payment, legal or audit purposes.	Ulearn may be unable to contract, pay or complete compliance checks.

9. How Ulearn collects information

- Directly from individuals when they complete forms, create an account, apply for a course, upload documents, contact Ulearn, attend events, respond to surveys, apply for a role, work with Ulearn or communicate with Ulearn.
- Automatically when individuals use Ulearn websites, apps and online services, including through cookies, analytics tools, security logs and similar technologies.

- From universities, colleges, schools, training providers, recruiters, employers, agents, referees, verification providers, service providers and business partners where relevant and lawful.
- From publicly available sources, such as professional profiles or institutional websites, where relevant and lawful.

10. Purposes and lawful bases

Ulearn will only use personal information where it has a lawful basis under UK GDPR. The lawful basis depends on the specific context. Where Ulearn relies on legitimate interests, it will maintain a legitimate interests assessment where appropriate. Where special category data or criminal offence information is used, a separate Article 9 condition or Article 10 / Data Protection Act 2018 condition must also apply.

Purpose	Examples of processing	Main lawful basis / bases
General enquiries and account creation	Responding to enquiries, creating user records, verifying contact details, managing preferences and providing requested information.	Contract or steps before contract; legitimate interests.
Course search and recommendations	Understanding profile, preferred subject, location, budget, mode of study, qualifications and eligibility to suggest relevant course options.	Contract or steps before contract; legitimate interests. PECR consent where profiling depends on non-essential cookies, pixels, tags, local storage or similar technologies.
Admissions support and application management	Preparing, checking and submitting applications, liaising with universities/colleges, tracking outcomes, arranging interviews/tests and managing evidence.	Contract or steps before contract; legitimate interests; legal obligation where applicable.
Document handling and verification	Receiving, storing, checking and forwarding passports, certificates, transcripts, CVs, references, English-language evidence and proof of funding.	Contract or steps before contract; legitimate interests; legal obligation where applicable. Avoid retaining identity documents longer than necessary.
Referrals to partner institutions, recruiters, agents or employers	Sharing relevant information at the individual's request or where necessary to progress a course, placement, recruitment or training opportunity.	Contract or steps before contract; legitimate interests; consent where required by the context.
Visa, immigration and right-to-study support	Processing passport, nationality, visa, immigration, proof-of-funding or residency information where relevant.	Contract or steps before contract; legal obligation; legitimate interests; Article 9/DPA 2018 condition where applicable.

Safeguarding, wellbeing and reasonable adjustments	Handling health, disability, accessibility, risk, safeguarding or support information to protect individuals or arrange support.	Legal obligation; legitimate interests; vital interests in emergencies; Article 9 condition such as explicit consent, vital interests, employment/social protection, legal claims or substantial public interest where documented.
Student support and service administration	Managing appointments, progress updates, communications, complaints, support requests, feedback and application follow-up.	Contract; legitimate interests; legal obligation.
Recruitment and candidate assessment	Reviewing CVs, interviews, assessments, references, right-to-work checks, role suitability, offer management and onboarding.	Contract or steps before contract; legal obligation; legitimate interests; Article 9/DPA 2018 where needed.
Employee, worker and contractor administration	Contracts, payroll, tax, pension, benefits, absence, performance, training, disciplinary, grievance, health and safety, IT access, expenses and emergency contacts.	Contract; legal obligation; legitimate interests; Article 9/DPA 2018 conditions where relevant.
Marketing and business development	Sending newsletters, offers, event invitations, course updates, partner opportunities and measuring engagement.	Consent; legitimate interests where PECR permits; legal obligation/legitimate interests for suppression records.
Website, app, cookies and analytics	Operating the website/app, maintaining security, remembering preferences, measuring usage, improving forms and services.	Legitimate interests or contract for essential services/security; PECR consent for non-essential cookies/storage unless an exemption applies.
Automated course matching and profiling	Using profile, preferences and interaction data to rank or suggest courses or content.	Legitimate interests; contract/steps before contract. PECR consent where profiling depends on non-essential storage/access technologies.
Events, webinars and surveys	Registering attendees, managing attendance, sending joining instructions, collecting feedback, running campaigns and follow-up.	Contract or steps before contract; legitimate interests; consent for optional marketing, prominent photos,

		recordings or testimonials where required.
Supplier, partner and professional adviser management	Due diligence, contracts, invoicing, payments, service management, audits, insurance and legal/professional advice.	Contract; legal obligation; legitimate interests.
Legal, regulatory, fraud prevention and complaints	Responding to lawful requests, maintaining records, preventing misuse, handling complaints, establishing or defending legal claims.	Legal obligation; legitimate interests; recognised legitimate interests where applicable; Article 9/DPA 2018 where sensitive/criminal offence data is involved.

11. Legitimate interests standard

Where Ulearn relies on legitimate interests, it will consider the purpose, necessity and impact of the processing before relying on this basis. The right to object applies to processing based on legitimate interests. For direct marketing, the right to object is absolute.

Legitimate interest	Examples	Safeguards
Providing and improving education-related services	Course search, admissions support, application tracking, service quality and user experience improvements.	Use only relevant data, restrict access, allow objections where applicable, avoid sensitive data unless a separate condition applies.
Partner and referral communications	Communications with universities, colleges, recruiters, agents and employers to progress a requested opportunity.	Share only necessary information, record the purpose, clarify when the recipient is an independent controller.
Security and fraud prevention	Monitoring suspicious activity, protecting systems, preventing misuse and maintaining audit logs.	Proportionate monitoring, limited access, defined retention, incident response procedures.
Lawful marketing	Relevant course updates, events and business-to-business communications where lawful.	PECR compliance, opt-outs, suppression lists, no under-18 marketing profiling.
Employment and workforce administration	Management, workplace systems, performance, health and safety, disputes and business continuity.	Transparency, role-based access, HR retention rules, proportionality review.
Business governance	Audits, finance, supplier management, quality assurance, dispute handling and legal claims.	Limit data to what is necessary, retention controls, need-to-know access.

12. Consent, cookies and PECR

Where Ulearn relies on consent, the individual can withdraw consent at any time. Withdrawal does not affect processing that took place before consent was withdrawn. Consent may be used for optional marketing, non-essential cookies and similar technologies, event photographs or recordings, some survey activity, social media linking, or explicit consent for certain special category data where appropriate.

For cookies and similar technologies, PECR consent is normally required before Ulearn stores information on, or accesses information from, a user's device through non-essential cookies, analytics cookies, marketing cookies, pixels, tags, local storage or similar technologies, unless a specific PECR exemption applies. UK GDPR legitimate interests may be relevant to later processing of personal information collected through those technologies, but legitimate interests does not replace PECR consent for non-essential cookie/storage access.

13. Special category data and criminal offence information

Special category data includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health, sex life or sexual orientation. Criminal offence information includes information about criminal convictions, offences, allegations, proceedings, security measures and related outcomes.

Ulearn will not ask for special category data or criminal offence information unless it is necessary for a specific service, legal requirement, safeguarding purpose, support arrangement, immigration/admissions process, employment administration or recruitment check. Ulearn must identify and document an Article 6 lawful basis and a specific Article 9 condition or Article 10 / Data Protection Act 2018 condition before processing.

Context	Likely data	Conditions and safeguards
Reasonable adjustments, disability or learning support	Health, disability, accessibility or support needs.	Article 9(2)(a) explicit consent where appropriate; Article 9(2)(b) where employment/social protection applies; Article 9(2)(g) only with a documented DPA 2018 Schedule 1 condition. Safeguards: restricted access, minimisation, secure storage and retention review.
Safeguarding or urgent welfare concerns	Health, wellbeing, risk, incident or emergency contact information.	Article 9(2)(c) vital interests for emergencies; Article 9(2)(g) substantial public interest only with documented Schedule 1 condition. Safeguards: need-to-know sharing, incident records, senior review.
Equality, diversity and monitoring	Racial or ethnic origin, religion, disability or other diversity data.	Explicit consent where optional; substantial public interest only where lawfully required and documented. Safeguards: optional collection where possible, aggregation, access restriction.
Admissions, visa, placement or	Health, disability, criminal offence,	Article 9(2)(a), 9(2)(b), 9(2)(f) or 9(2)(g) depending on context. Criminal offence

professional-suitability checks	professional suitability, passport or immigration-related information.	data only where authorised by law and a DPA 2018 Schedule 1 condition applies.
Recruitment and employment checks	Health, disability, right-to-work, equality monitoring, DBS/criminal record information where role-relevant.	Article 9(2)(b), explicit consent where genuinely optional, legal claims or substantial public interest where documented. Criminal offence data only where authorised by law.
Legal claims, complaints or regulatory matters	Any relevant sensitive or criminal offence information included in the matter.	Article 9(2)(f) legal claims or Article 9(2)(g) where supported; DPA 2018 conditions for criminal offence data.

Where Ulearn relies on a DPA 2018 Schedule 1 condition that requires one, it must maintain an Appropriate Policy Document explaining procedures for complying with the UK GDPR principles and retention/erasure arrangements for special category and criminal offence data.

14. Automated course matching, profiling and decision-making

Ulearn may use information such as course interests, qualifications, location, budget, preferred study mode, engagement with the website/app and application status to suggest courses, prioritise information, personalise content or improve services. Course suggestions, eligibility indicators and ranked results support human advice and user choice. They do not guarantee admission, funding, visa approval or enrolment.

Ulearn will not make decisions based solely on automated processing that produce legal or similarly significant effects unless it tells individuals separately, explains the logic involved, explains the significance and expected consequences, and provides safeguards such as human review, the ability to express a view and the ability to challenge the decision.

15. Sharing personal information

Recipient category	Examples	Reason for sharing
Universities, colleges, schools and training providers	Partner institutions and other providers where applicable. Confirm current partners before naming publicly.	Course search, applications, admissions, enrolment, student support and related communications.
Admissions and education-sector bodies	UCAS, awarding bodies, professional bodies, Office for Students or equivalents where applicable.	Admissions, reporting, regulatory compliance, verification or sector requirements.
Immigration and public authorities	Home Office, embassies, consulates or other authorities where applicable.	Visa, right-to-study, immigration, safeguarding, legal or regulatory requirements.

Funding, finance and student support bodies	Student Loans Company, scholarship bodies, sponsors, employers or funding partners.	Funding assessment, scholarship administration, payment support or sponsorship.
Recruiters, employers, agents and intermediaries	Education agents, recruitment partners, placement providers, employers, referees or intermediaries.	Referral, placement, recruitment, work-based learning or requested opportunity support.
Technology and service providers	Cloud hosting, CRM, email, analytics, call handling, document management, IT support, security, payment, marketing, HR/payroll and communications providers.	Operating and improving services, secure storage and business operations.
Verification and screening providers	Identity, qualification, right-to-work, reference, DBS or background-check providers.	Verification, safeguarding, suitability, fraud prevention or legal compliance.
Professional advisers and insurers	Lawyers, accountants, auditors, consultants, insurers and debt recovery providers.	Legal advice, audit, insurance, finance, claims, disputes and governance.
Regulators, courts and law enforcement	ICO, courts, police, HMRC, Companies House, regulators and public authorities.	Legal obligation, lawful request, claims, fraud prevention, safeguarding or regulatory compliance.
Corporate transaction parties	Potential buyers, investors, acquirers, advisers or restructuring parties.	Business sale, merger, restructuring, due diligence or transfer of assets, subject to safeguards.

16. International transfers

Ulearn generally aims to store and process personal information in the United Kingdom or European Economic Area where possible. However, Ulearn has international contacts and may use service providers or partners that process information in other countries. Where personal information is transferred internationally, Ulearn will use appropriate safeguards required by law, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to EU Standard Contractual Clauses, contractual protections, technical and organisational safeguards, data minimisation, pseudonymisation or anonymisation where appropriate. Ulearn should identify likely transfer countries, providers and safeguards in internal records and provide more information on request.

17. Retention schedule

Ulearn will keep personal information only for as long as necessary for the purposes for which it was collected, including legal, accounting, reporting, safeguarding, regulatory, audit and dispute-resolution requirements. The periods below are default periods unless a longer or shorter period is required by law, contract, safeguarding, investigation, dispute, regulator requirement or legal advice.

Record type	Default retention period	Notes

General enquiries where no application is made	Up to 2 years after last meaningful contact.	May be shorter where the enquiry is resolved and no further relationship exists.
Account/profile information	While account is active, then up to 2 years after closure or last activity.	Longer if required for disputes, audit, safeguarding or legal claims.
Course-search records and advice notes	Up to 3 years after last contact or completion of support.	Used for continuity, quality assurance and applicant support.
Application records submitted to institutions	Up to 6 years after application outcome or end of Ulearn support.	Partner institutions retain their own records separately.
Uploaded documents including passport, certificates, transcripts, CV, proof of funding and English-language evidence	Normally delete or anonymise within 12 months after application outcome or service completion unless needed for legal, audit, complaint or regulatory reasons.	Record verification status where possible rather than keeping full copies.
Visa / immigration support records	Up to 6 years after relevant support activity, unless a shorter period is appropriate or a longer legal/regulatory period applies.	Retain only necessary records and avoid unnecessary identity-document copies.
Safeguarding, serious complaint or legal-claim records	Up to 6 years after closure, or longer where required by law, safeguarding risk, insurer, regulator or legal advice.	Access-restricted and periodically reviewed.
Disability, health, accessibility or reasonable-adjustment information	For the duration of the support/application/employment need plus up to 12 months unless needed for legal, safeguarding, complaint or institutional requirements.	Review necessity regularly and share on a need-to-know basis.
Marketing consent and preference records	While subscribed and for up to 2 years after last engagement; suppression records retained as long as necessary to respect opt-outs.	Suppression records should contain minimal information.
Website analytics data	Up to 26 months by default, or as stated in the cookie tool/analytics settings.	Anonymise or aggregate where possible.
Cookie consent records	Up to 12 months, then refreshed where required.	Exact period depends on cookie management tool.
Security logs	Up to 12 months unless needed for investigation, fraud prevention or legal/security incident response.	Access restricted to authorised technical/security staff.

Recruitment candidate records - unsuccessful applicants	Up to 12 months after recruitment decision, unless consent is obtained for longer talent-pool retention.	Right-to-work/sensitive checks should not be retained unnecessarily.
Employee, worker and contractor personnel records	Employment/engagement duration plus up to 6 years after termination unless another statutory, pension, immigration, safeguarding or claims period applies.	Maintain separate staff retention rules where needed.
Payroll, tax, pension and finance records	Usually 6 years from the end of the relevant financial year, or longer where pension/statutory rules require.	Subject to accounting, tax and pension requirements.
Supplier and partner contract records	Contract duration plus 6 years.	Legal, finance, audit and contract limitation purposes.
Invoices, accounting and tax records	Usually 6 years from the end of the relevant financial year.	Subject to accounting and tax requirements.
Event attendance records	Up to 2 years after event unless needed for contracts, safeguarding, claims or follow-up consent.	Campaign-specific notices may set shorter periods.
Survey responses	Up to 2 years, or anonymised earlier where possible.	Anonymous data may be retained longer if individuals cannot be identified.

18. Individual rights

Right	Meaning
Right to be informed	To receive clear information about how Ulearn collects and uses personal information.
Right of access	To request a copy of the personal information Ulearn holds.
Right to rectification	To ask Ulearn to correct inaccurate or incomplete personal information.
Right to erasure	To ask Ulearn to delete personal information in certain circumstances.
Right to restrict processing	To ask Ulearn to limit how personal information is used in certain circumstances.
Right to data portability	To receive certain personal information in a structured, commonly used and machine-readable format, or ask Ulearn to transfer it to another controller, where the right applies.
Right to object	To object to processing based on legitimate interests, public task or direct marketing. For direct marketing, this right is absolute.
Rights related to automated decision-making	To not be subject to certain decisions based solely on automated processing that produce legal or similarly significant effects unless permitted by law and safeguards apply.

Right to withdraw consent	To withdraw consent where consent is the lawful basis.
Right to complain	To complain to Ulearn or to the Information Commissioner's Office.

Requests should be sent to admin@ulearn.education. Ulearn may ask for proof of identity or authority where a request is made through a representative. Ulearn usually responds within one month and may extend by up to two further months for complex requests where the law allows.

19. Security

- Encryption and secure transmission where appropriate.
- Role-based access controls, authentication and need-to-know permissions.
- Confidentiality obligations for staff, contractors and service providers.
- Staff training and internal data protection policies.
- Secure hosting, storage, backup and document-management arrangements.
- Monitoring, logging and incident response procedures.
- Periodic review of information collection, storage and processing practices.
- Supplier due diligence and written data protection terms where appropriate.
- Assessment and notification of personal data breaches to the ICO and affected individuals where legally required.

20. Third-party websites and services

Ulearn's website, app or communications may contain links to third-party websites, services or content. Ulearn is not responsible for the privacy practices of those third parties. Individuals should read their privacy notices before providing personal information to them.

21. Changes to this policy

Ulearn may update this policy to reflect changes in services, legal requirements, ICO guidance, suppliers or processing activities. The latest version should be available on the website or provided on request. Where changes are significant, Ulearn will take reasonable steps to bring them to the attention of affected individuals.

22. Complaints

Individuals can contact Ulearn first if they have concerns about how personal information is used. They also have the right to complain to the Information Commissioner's Office at any time: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; website https://ico.org.uk; telephone 0303 123 1113.