



## LINK EDUCATION LTD

P024 – PRIVACY POLICY

VERSION 2.0 | AUGUST 2026 | CONTROLLED DOCUMENT

## 1 PURPOSE, STATUS AND SCOPE

This policy sets the governance requirements supporting Link Education Ltd's public privacy information. It explains how personal data must be collected, used, shared, retained and protected across recruitment, safeguarding, employment, payroll, client services and website operations. The public-facing Privacy Notice gives individuals the transparency required by UK data-protection law.

It applies to directors, employees, consultants, contractors and processors and to data about applicants, candidates, agency workers, employees, client contacts, referees, website users, suppliers and other business contacts. It must be read with P005 and P021; those policies contain the detailed security and retention controls.

## 2 CONTROLLER AND CONTACT DETAILS

- Controller: Link Education Ltd, 3a Victoria Works, 6 Fairway, Petts Wood, Kent BR5 1EG.
- Telephone: 01689 878565.
- Privacy contact: enquiries@link-education.co.uk.
- ICO registration number: Z7313888.

## 3 DATA-PROTECTION PRINCIPLES

- Process personal data lawfully, fairly and transparently.
- Collect it for specified, explicit and legitimate purposes.
- Use only data that is adequate, relevant and necessary.
- Keep it accurate and correct errors without undue delay.
- Retain it only for an approved period and securely dispose of it.
- Protect confidentiality, integrity and availability through proportionate controls.
- Be able to demonstrate compliance through records, decisions and oversight.

## 4 INFORMATION PROCESSED

| Category                      | Examples                                                                                                                              |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Identity/contact              | Names, previous names, address, email, telephone, date of birth, photograph, National Insurance number and emergency contact.         |
| Recruitment/work              | CV, application, work history, gaps, availability, preferences, interviews, assignments, performance, attendance and communications.  |
| Compliance                    | Identity and right-to-work evidence, references, qualifications, TRA/EWC or professional status, training and online-search outcomes. |
| Safeguarding/criminal offence | DBS and Update Service details, barred-list results, overseas checks, allegations, concerns, referrals, outcomes and risk decisions.  |
| Health/equality               | Medical fitness, disability, adjustments, statutory leave and optional equality-monitoring information.                               |
| Payroll/pension               | Bank, tax, pay, timesheets, holiday, statutory deductions, pension and attachment information.                                        |
| Clients/suppliers             | Business contact, role, organisation, bookings, contracts, invoices, service and complaint records.                                   |
| Website/technical             | Forms, account details, IP address, device/browser, logs, cookie choices and site interactions.                                       |

## 5 SOURCES

- The individual, including applications, registration, interviews, forms, calls, emails and website use.
- Clients, former employers, referees and authorised representatives.
- Job boards, CV databases and professional networking services used under their terms and applicable law.
- DBS, Home Office services, TRA, EWC, professional bodies, Companies House and other official sources.
- Public online sources where a proportionate safer-recruitment or due-diligence check is lawful and notified.
- Payroll, pension, IT, website and other approved service providers.
- Police, local authorities, LADO, regulators, courts or other bodies where disclosure or receipt is lawful.

## 6 PURPOSES AND LAWFUL BASES

| Purpose                                                        | Typical lawful basis                                                                                                |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Provide work-finding, recruitment and placement services       | Steps at the individual's request before contract; contract; legitimate interests.                                  |
| Employ, engage, pay and administer workers                     | Contract; legal obligation; legitimate interests.                                                                   |
| Vetting, right to work, safeguarding and suitability           | Legal obligation; legitimate interests; substantial public-interest conditions for sensitive/criminal-offence data. |
| Client service, contracts, bookings and billing                | Contract; legitimate interests; legal obligation.                                                                   |
| Complaints, investigations, audit, fraud prevention and claims | Legal obligation; legitimate interests; legal claims and substantial public interest where applicable.              |
| Health, adjustments and statutory leave/pay                    | Legal obligation and employment/social-protection conditions; explicit consent only where genuinely appropriate.    |
| Vacancy alerts and business marketing                          | Consent where required by PECR; otherwise legitimate interests with a clear right to object.                        |
| Website operation, security and analytics                      | Legitimate interests for necessary operation/security; consent for non-essential cookies.                           |

Consent is not used where another basis is more appropriate and is never made a condition of an unrelated service. Public task is used only where Link itself is legally entitled to rely upon it. Each process must have an Article 6 basis and, for special-category or criminal-offence data, the additional applicable condition and safeguards.

## 7 SPECIAL-CATEGORY AND CRIMINAL-OFFENCE DATA

Sensitive data is processed only where necessary, proportionate and supported by an Article 9 or Data Protection Act 2018 condition. Criminal-offence, DBS and safeguarding data is subject to Article 10 and Schedule 1 controls, Link's Appropriate Policy Document where required, restricted access and P002 decision-making standards.

- Record only the information necessary for the check, decision, safeguarding response or legal requirement.
- Separate allegation, evidence, finding, outcome and risk decision; do not present unsubstantiated information as fact.
- Do not retain DBS certificates or detailed criminal information beyond the justified period.
- Share safeguarding or criminal-offence information only with an authorised recipient and on a lawful, need-to-know basis.
- Keep equality monitoring separate from selection decisions wherever practicable.

## 8 SHARING AND PROCESSORS

Link does not sell personal data. Relevant information may be shared with schools, nurseries, MATs and other hirers; payroll, pension, banking, IT, hosting and communications providers; DBS, HMRC, Home Office, TRA, EWC, TPR and regulators; local authorities, LADO, police, courts and safeguarding bodies; and insurers, auditors, legal or HR advisers. The minimum necessary information is shared for the stated purpose.

Processors must be approved, subject to written Article 28 terms, confidentiality, security, breach, deletion and sub-processing controls. Client disclosure of candidate information must follow the recruitment purpose, data-minimisation rules and any required candidate information.

## 9 INTERNATIONAL TRANSFERS

Where personal data is transferred outside the UK, the owner must confirm a lawful transfer mechanism, such as UK adequacy regulations, the International Data Transfer Agreement or UK Addendum, and complete a transfer-risk assessment where required. Supplementary security measures must be applied where appropriate. Individuals are not asked to "consent" merely to legitimise routine supplier transfers.

## 10 RETENTION AND SECURITY

P021 contains the controlled retention schedule. Data is kept only for a documented legal, safeguarding, contractual, claims or operational purpose, subject to holds. At the end of the period it is securely destroyed or

irreversibly anonymised. Backups are managed through controlled rotation and are not used as an indefinite archive.

- Use approved systems, role-based access, strong authentication and secure transfer methods.
- Do not store company data in personal email, devices, messaging accounts or unapproved cloud/AI services.
- Verify recipients and minimise attachments before sending personal data.
- Report loss, misdirection, unauthorised access or other suspected breach immediately under P005.
- Apply enhanced access and audit controls to safeguarding, health, criminal, payroll and identity data.

## 11 INDIVIDUAL RIGHTS

- To be informed about processing.
- Access to personal data and supplementary information.
- Rectification of inaccurate or incomplete data.
- Erasure where the legal conditions apply.
- Restriction of processing in applicable circumstances.
- Data portability for qualifying automated processing based on consent or contract.
- Objection, including an absolute right to object to direct marketing.
- Safeguards concerning solely automated decisions producing legal or similarly significant effects.
- Withdrawal of consent at any time where consent is relied upon.
- Complaint to the Information Commissioner's Office.

Rights are not absolute. Requests must be logged, identity verified proportionately and answered without undue delay, normally within one month. No fee is normally charged; any extension, refusal or fee must meet the statutory test and be authorised by the COO.

## 12 COOKIES, MARKETING AND AUTOMATION

- Non-essential cookies or similar technologies are activated only after valid consent and can be rejected as easily as accepted.
- The website cookie information must identify categories, purposes, providers and durations and reflect the technologies actually deployed.
- Electronic marketing follows PECR and privacy preferences; each relevant message provides a simple opt-out.
- Suppression records may be retained to honour an objection.
- Link does not make recruitment or employment decisions solely by automated means where the decision has legal or similarly significant effects. Human review is required for matching, screening or AI-assisted outputs.

## 13 TRANSPARENCY AND CHANGE CONTROL

Privacy information must be concise, accessible and supplied at or before collection, or within the applicable period where data comes from another source. Candidate, employee, client, website, cookie and form notices must remain consistent with actual processing. A new or materially changed process, system, supplier, data use or transfer requires privacy review and, where high risk is likely, a DPIA before implementation.

## 14 COMPLAINTS, BREACHES AND ASSURANCE

Privacy concerns should be sent to [enquiries@link-education.co.uk](mailto:enquiries@link-education.co.uk). Link will investigate fairly and explain the outcome. Individuals may complain to the ICO at [ico.org.uk](https://ico.org.uk) or 0303 123 1113. This does not affect other legal rights.

The COO oversees rights requests, breaches, DPIAs, processor assurance, retention exceptions and privacy-notice reviews. Compliance is sampled through audit, complaints, access reviews, training, incident trends and website checks. Deliberate misuse or concealment may result in disciplinary or contractual action and regulatory reporting.

## 15 RELATED CONTROLLED DOCUMENTS

- P001 – Safeguarding & Child Protection Policy
- P002 – Recruitment, Selection & Vetting Policy
- P005 – GDPR, Data Protection & Information Security Policy
- P007 – Complaints & Escalation Procedure
- P009 – Equality, Diversity & Inclusion Policy
- P013 – Whistleblowing Policy
- P019 – Code of Conduct & Ethics Policy
- P021 – Data Retention & Secure Disposal Policy
- P022 – Workplace Pension Policy
- P023 – Advertising & Vacancy Promotion Policy
- P025 – Customer Service Policy
- Appropriate Policy Document, privacy notices, cookie information, DPIAs, processor contracts and breach/rights registers

## 16 DOCUMENT CONTROL

| Field            | Controlled information                                               |
|------------------|----------------------------------------------------------------------|
| Document title   | Privacy Policy                                                       |
| Reference        | P024                                                                 |
| Version          | 2.0                                                                  |
| Effective date   | August 2026                                                          |
| Review date      | August 2027                                                          |
| Owner            | Chief Operating Officer / Data Protection Lead                       |
| Approved by      | Managing Director                                                    |
| Review frequency | Annually or sooner following legal, ICO, system or processing change |
| Status           | Controlled document – active                                         |
| Supersedes       | Previous P024 Privacy Policy                                         |