In2Ed – Data Protection and Retention Policy

Company: In2Ed | **Version:** 2.0 | **Revision date:** 19 November 2026

Policy owner: Data Protection Lead – Josh Hamlington, josh@in2ed.co.uk.

Approved by: Josh Hamlington.

Approval and effective date: 19 November 2026

Next review: 19 November 2027, or sooner following legal or operational changes.

This policy supersedes the Data Retention Policy dated 5 October 2026 with effect from 19 November 2026. Publication, staff communication and system implementation must be evidenced; policy approval does not certify that those actions have occurred.

1. Purpose

This policy sets mandatory requirements for collecting, using, sharing, securing, retaining and disposing of personal data in recruitment, worker supply, employment and business administration. It addresses the seven principles in Article 5 of the UK GDPR, alongside the Data Protection Act 2018 and applicable amendments, and record-keeping obligations under the Conduct of Employment Agencies and Employment Businesses Regulations 2003. It must be read alongside the relevant privacy notices and safeguarding procedures.

2. Scope

This policy applies to:

- All In2Ed employees, consultants, temporary workers, and representatives
- All personal data relating to candidates, agency workers, clients, schools, staff, suppliers, and partners
- All systems, platforms, devices, and communication channels used to process personal data (email, CRM, messaging apps, cloud storage, etc.)

3. Data Protection Principles

In2Ed must apply all seven principles to every stage of the personal-data lifecycle:

1. **Lawfulness, fairness and transparency:** identify and record a valid lawful basis before processing; explain the processing clearly in an appropriate privacy notice; do not use data in misleading or unjustifiably harmful ways.

2. **Purpose limitation:** collect data for specified, explicit and legitimate purposes. Assess and document whether any proposed new use is compatible or requires a separate lawful basis and updated information to individuals.
3. **Data minimisation:** collect, disclose and retain only information necessary for the identified purpose. Separate legally required records from optional recruitment material and unnecessary duplicates.
4. **Accuracy:** take reasonable steps to verify information, keep it current where necessary, record the source and correct or remove inaccurate information without delay.
5. **Storage limitation:** apply the category-specific schedule below, record the relevant trigger and disposal date, review necessity regularly and delete or irreversibly anonymise information when no longer needed.
6. **Integrity and confidentiality (security):** protect against unauthorised or unlawful processing and accidental loss, destruction or damage through appropriate organisational and technical controls.
7. **Accountability:** maintain evidence of lawful bases, privacy information, retention decisions, access controls, training, rights requests, breaches and disposal. The Data Protection Lead oversees compliance and reports unresolved risks to management.

4. Retention Periods

4.1 How retention decisions are made

There is no blanket six-year retention rule for a candidate, worker or client file. A minimum period protects only the records needed to meet that obligation, not every item held about the person. Longer periods in this schedule that are In2Ed policy choices remain subject to necessity, proportionality and individual rights.

For records required by regulation 29 of the Conduct Regulations, retain records for at least one year from creation. For the required work-seeker and hirer application particulars, also retain them for at least one year after In2Ed last provides recruitment or work-finding services to that work-seeker or hirer. Apply whichever expiry is later. This includes work-seekers who have never been placed where In2Ed has taken action to find them work. The trigger is the last service, not simply the last assignment or last database update.

Record the last-service date and its supporting evidence, employment/engagement end date where relevant, record category, lawful basis, applicable minimum, review date and disposal date. If several rules apply to the same necessary record, retain it until the latest applicable expiry. Do not extend unrelated material simply because it shares a file or system.

4.2 Retention schedule

Record category	Retention period and trigger	Application and disposal rule
Work-seekers: required registration and service records	Keep during service and until the later of one year from record creation or one year after last work-finding service.	Includes required terms and changes, qualifications, training/experience, relevant enquiries, introductions and engagement details. Applies where action is taken, whether or not an assignment results. Delete optional or duplicate material earlier when no longer necessary.
Clients/hirers: required application and service records	Keep during service and until the later of one year from record creation or one year after last service to that hirer.	Retain the particulars and relevant service evidence required by the Conduct Regulations securely. Separate these from financial records with longer obligations.
Speculative CVs/applications on which no action is taken	Assess on receipt; delete promptly if not needed and no other lawful basis exists.	The Conduct Regulations do not require retention of application particulars where no action is taken. Any talent-pool use requires a documented lawful basis, transparent notice and review date; it must not create indefinite retention.
Right-to-work evidence for workers employed/engaged by In2Ed, including assigned workers	For the duration of the relevant employment/engagement and at least two years after it ends; also honour any later applicable Conduct Regulations expiry.	Record check evidence and dates securely. The end of a single assignment does not start the clock if employment/engagement continues. Delete after the applicable period unless a separately documented lawful requirement justifies further retention. Confirm responsibility and applicable requirements

		for other supply-chain arrangements.
Payroll, pay history, timesheets and minimum-wage evidence for assigned workers and internal staff	In2Ed standard: six years after the end of the relevant tax year, but never less than the applicable statutory minimum. Minimum-wage evidence: at least six years beginning with the day the following pay reference period ends.	PAYE alone generally requires three years from the end of the relevant tax year; it is not a universal six-year HMRC rule. Retain the pay, hours and supporting evidence needed for minimum-wage compliance. Finance must apply any later accounting or other mandatory expiry to the relevant records only.
Invoices, statements, remittances and accounting records	In2Ed standard: six years after the end of the financial year to which the record relates; longer where a documented applicable requirement or live enquiry requires it.	Finance must confirm the statutory tax/accounting rules applicable to the business before approval and record any later expiry. Remove unrelated personal information and unnecessary copies.
Contracts and essential evidence for legal claims	In2Ed standard: up to six years after the relevant contract or employment ends, where necessary and justified; assess any different limitation period individually.	A claims-related policy period is not an automatic duty to keep a complete recruitment or HR file. Record the purpose, lawful basis and necessity; assess erasure requests individually.
References, qualifications, recruitment ID and training evidence	Apply the required work-seeker minimum where the record forms part of the mandatory recruitment record. Review other copies when their purpose ends.	Do not routinely retain all ID or reference material for six years. Apply the separate right-to-work rule where applicable, or record a specific ongoing safeguarding, contractual or other lawful need.
DBS certificate information and copies	Retain only as long as necessary after the recruitment or other relevant decision, under the DBS handling rules; no automatic six-year period.	The Data Protection Lead must document the necessity, permitted retention and review date, including any justified safeguarding-audit requirement. Destroy certificate contents and

		copies when no longer needed. A minimal check record may be retained separately: issue date, subject, check type, role, reference number and recruitment decision.
Safeguarding concerns, allegations, referrals and related complaints	Case-specific period approved by the safeguarding lead and Data Protection Lead, reflecting applicable guidance, outcome, legal duties and any preservation notice.	Do not apply blanket indefinite retention. Before issue, document the applicable category rules, triggers and expiry/review dates in a controlled safeguarding schedule, obtaining specialist advice where required. No destruction while a lawful investigation or preservation hold applies.
Other internal HR, disciplinary and training records	Review during employment and on leaving. Essential contractual evidence: as above. In2Ed default for non-safeguarding disciplinary records: review at two years after case closure and delete unless a documented need remains.	Remove expired warnings from active decision-making in accordance with HR procedures. Keep only necessary evidence; safeguarding, pay and other specialist records follow their own rules.
Audit trails and system-access logs	In2Ed defaults: compliance audit trails up to six years from creation; routine system-access logs up to one year from creation, subject to documented necessity.	The Data Protection Lead must justify the selected period and minimise identifiable content. Incident evidence may be preserved under a specific hold; routine logs must not be kept longer without justification.
Email, SMS, WhatsApp, downloads and local copies	Transfer necessary business evidence promptly into the approved secure record system, verify completeness, then delete unnecessary channel/local copies.	The retained business record follows its category above. Do not delete the only copy of required evidence or material under a hold. Staff departure does not shorten statutory retention.

Rights-request, breach, deletion and retention-decision logs	In2Ed standard: up to six years after closure, subject to necessity review; retain only minimal accountability evidence.	Do not retain the complete erased file merely to prove that it was erased. Record the request/decision, reasons, actions, responsible person and completion/review dates.

4.3 Reviews, exceptions and legal holds

The Data Protection Lead must coordinate a documented retention review at least quarterly and when a service ends, a request is received or a hold is released. Delete or irreversibly anonymise expired records promptly following approval; do not wait for the annual policy review.

Any extension must identify the specific records, lawful purpose and basis, applicable legal requirement or claim, access restrictions, approver and next review or disposal date. A general possibility of future work, a client preference or the phrase “for audit” is not sufficient on its own. Review holds at least quarterly and dispose of records when the hold ends and no other lawful retention requirement remains.

5. Secure Storage

Personal data must be held in approved, access-controlled systems. In2Ed requires the following controls, with implementation evidence retained by the responsible system owner:

- Encryption appropriate to the risk, secure transfer methods, strong passwords, multi-factor authentication where available, device protection, updates and tested recovery arrangements.
- Role-based, least-privilege access; separate restrictions for identity documents, payroll, health, DBS and safeguarding records; access reviews at least quarterly and whenever roles change.
- Locked storage and controlled access for paper records, and secure arrangements for home working, transport and confidential disposal.
- No personal devices, personal email accounts or unapproved messaging/cloud services unless specifically authorised, necessary and covered by documented security and deletion controls.
- Authorised and proportionate sharing only: verify the recipient and purpose, disclose the minimum required, and record sensitive disclosures. Put appropriate written data-protection terms in place with service providers and confirm responsibilities when sharing with schools and clients.
- Before using a provider or transferring personal data outside the UK, the Data Protection Lead must assess security, access, location, lawful transfer

requirements, retention and deletion arrangements. Assess higher-risk processing before it starts and document any required impact assessment.

Before collecting health or other special-category information or criminal-offence information, document the additional processing conditions and safeguards that apply. Do not assume ordinary consent to recruitment permits every use or disclosure. Keep any required supporting policy documentation separately.

6. Secure Deletion

Delete or irreversibly anonymise data once its purpose and applicable retention requirements end, including where a valid erasure request requires earlier deletion. First check the record category, all applicable minima and any specific legal or safeguarding hold. Removing a record from view or revoking access is not the same as deleting it.

- Remove authorised records from the CRM, cloud storage, email, messaging, downloads, device copies and recoverable deleted-item locations where practicable; obtain deletion confirmation from processors where required.
- Use secure erasure for digital media and confidential shredding or an approved destruction service for paper. Keep records secure while awaiting destruction.
- Where immediate removal from backups is not practicable, put the data beyond operational use, restrict access and allow it to expire through a documented backup cycle. Maintain a minimal deletion instruction so erased data is not reintroduced following restoration. Record the applicable backup expiry and verify the process with each provider.
- Maintain a disposal log recording category, date range or minimal record identifier, authority, method, approver and completion date; obtain supplier destruction evidence where relevant.

When staff leave, revoke their access promptly; recover devices and transfer required business records before removing local or personal-account copies. Obtain confirmation that In2Ed data has been removed from phones, email, messaging apps and other devices used for work, subject to preservation requirements. Do not destroy the only copy of a record that In2Ed must retain.

7. Data Subject Rights

Individuals may request access, rectification, erasure, restriction, objection and portability where applicable, and may withdraw consent where processing relies on it. They may also raise concerns about automated decisions where applicable and complain to the ICO. Staff must forward any verbal or written request immediately to

the Data Protection Lead, who must log it, verify identity proportionately where needed and coordinate the response.

7.1 Right to erasure (“right to be forgotten”)

The right is not absolute. A scheduled six-year period does not, by itself, justify refusing erasure. Equally, a request does not override a continuing legal obligation to retain particular records. Assess each category separately and delete information for which the right applies without undue delay.

1. Identify the request scope and locate records across live systems, archives, devices, messaging services and relevant processors. Record the receipt date and response deadline.
2. For each category, identify the current purpose, lawful basis, mandatory minimum and trigger. Consider whether the right to erasure applies and whether a specific exception, such as a legal obligation or the establishment, exercise or defence of legal claims, justifies retaining necessary information.
3. Erase optional or unnecessary recruitment information where required, even if payroll or right-to-work evidence must remain. For example, a former assigned worker may have unnecessary candidate-profile material erased while essential service records remain within the one-year minimum, right-to-work evidence remains within the applicable two-year post-engagement period, and minimum-wage/payroll evidence remains within the applicable six-year period. Each clock must be calculated from its own trigger in section 4.
4. For any retained records, document the specific reason and exception, minimum necessary content, restricted access, permitted use and review/disposal date. Do not continue matching, marketing or other unrelated use merely because records must be held for compliance. Assess any request for restriction separately.
5. Inform recipients of erasure where required, unless this is impossible or involves disproportionate effort, and coordinate processor action. Record actions taken and explain backup treatment where relevant.
6. Respond without undue delay and normally within one month of receipt. Any lawful extension or adjustment must be assessed and documented; notify the individual of an extension and reasons within the initial month. If refusing all or part of a request, explain the reasons, what is retained and why, the relevant period or criteria, and the right to complain to the ICO and seek a judicial remedy.

Keep only proportionate evidence of the decision and its completion. Do not retain an entire erased file for accountability purposes.

8. Breach Management

All suspected loss, unauthorised access, disclosure, alteration or destruction of personal data must be reported immediately to the Data Protection Lead. The Lead must coordinate containment and recovery, preserve necessary evidence, assess risks to individuals, document the decision on regulatory and individual notification, and make any required notifications within the applicable statutory deadlines. Record every breach, including those not notified, its consequences, remedial action and lessons learned. Staff must not delay escalation while investigating themselves.

9. Informing clients and work-seekers

In2Ed must make its commitment to data protection clear before or when it collects personal information. The following are mandatory communication requirements, not a statement that publication has already been completed:

- **Website:** publish the approved current policy and accessible privacy notices through a clearly labelled privacy/data-protection link. Include the policy version, review date and monitored contact route. Provide a copy on request and offer an accessible alternative where needed.
- **Work-seekers:** provide the relevant privacy notice and policy link during registration and before collecting supporting documents; include the link in registration confirmations and worker onboarding information.
- **Clients and schools:** provide the relevant privacy notice and policy link during client onboarding and with the terms of business or service confirmation. Explain responsibilities for any personal data shared.
- **Privacy-notice content:** identify the controller and contact details, purposes and lawful bases, relevant legitimate interests, information sources and categories where appropriate, recipients, relevant international transfers and safeguards, retention periods or criteria, rights and how to exercise them, and the ICO complaint route. Explain required information and consequences of not providing it, and any relevant automated decision-making. The policy does not replace these notices.
- **Changes and evidence:** communicate material changes where required. Keep dated publication evidence and notice versions, registration/onboarding templates and proportionate evidence showing when the relevant notice was provided. Receipt of a notice is not consent to all processing.

10. Responsibilities, review and audit readiness

Management must approve this policy and appoint a named Data Protection Lead with a monitored contact route. The Lead maintains the retention schedule and rights/breach logs; recruitment and client teams record last-service dates and provide

privacy information; Finance validates payroll, minimum-wage and accounting expiry rules; system owners implement access, backup and disposal controls; the safeguarding lead approves safeguarding retention requirements. All staff must follow this policy and complete appropriate induction and refresher training.

The Data Protection Lead must review the policy at least annually and sooner following legal changes, material operational changes, a significant incident or audit findings. Track changes, obtain approval, communicate revisions and preserve controlled policy versions.

11. Reference guidance

Official sources consulted on 19 November 2026. The Data Protection Lead must check for relevant changes when approving and reviewing this policy.

- ICO – A guide to the data protection principles
- ICO – Storage limitation
- ICO – Right to erasure
- ICO – UK GDPR guidance and resources
- Conduct of Employment Agencies and Employment Businesses Regulations 2003 – regulation 29
- Home Office – Right to work checks: an employer's guide
- HMRC – PAYE and payroll: keeping records
- HMRC – National Minimum Wage Manual: records
- DBS – Handling of certificate information