

Data Protection and Privacy Policy

A2A Qualifications Limited

Document reference	A2A-DP-POL-006
Version	1.1
Status	Published
Owner	Director
Approver	Director
Effective date	August 2026
Next review	10 June 2027 (annual), or earlier on change of legislation, systems or processing
Supersedes	A2A-DP-POL-006 v1.0 (10 June 2026); A2A Training Data Protection Policy V4 (6 October 2024) and all earlier versions.
Applies to	All A2A personnel, assessors, internal quality assurers, associates and staff who handle personal data; and all individuals whose personal data A2A processes, including apprentices and learners, staff, and contacts at centres, training providers and employers.

1. Purpose and scope

This policy sets out how A2A Qualifications Limited (“A2A”) collects, uses, shares, stores and protects personal data, and how it meets its obligations under the UK GDPR and the Data Protection Act 2018. It applies to all A2A personnel, assessors, internal quality assurers, associates and staff who handle personal data, and explains to individuals — apprentices and learners, staff, and contacts at centres, training providers and employers — how their personal data is handled.

It applies wherever the work is done, including at home and on personal equipment.

2. Who we are

A2A Qualifications Limited is the data controller for the personal data described in this policy. A2A is registered with the Information Commissioner’s Office (ICO), registration number ZB263774. Company number 11740930. Ofqual recognition RN6096; assessment organisation reference EPAO889.

Questions about this policy or about personal data can be sent to A2A’s data protection lead, Louise Warren (Director), at info@a2aqualifications.co.uk. A2A is not required to appoint a statutory Data Protection Officer and has not done so.

3. Regulatory and policy context

A2A processes personal data under the **UK GDPR** and the **Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025**, and is regulated by the ICO for data protection. The main data protection provisions of the 2025 Act took effect on 5 February 2026, with the statutory complaints duty at section 15 following on 19 June 2026.

As an Ofqual-recognised awarding organisation, A2A's assessment activity is also governed by the applicable **assessment plan** for each standard and by **Ofqual's recognition requirements**. Where any A2A internal policy or procedure differs from the applicable assessment plan or Ofqual's requirements, the assessment plan and Ofqual's requirements take precedence.

For context, the occupational standards and assessment plans are owned by Skills England; A2A is listed on the Apprenticeship Provider and Assessment Register (APAR); and responsibility for apprenticeships policy moved to the Department for Work and Pensions in September 2025.

Our data protection principles

A2A applies the principles set out in the UK GDPR. Personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes, and not used in incompatible ways;
- adequate, relevant and limited to what is necessary (data minimisation);
- accurate and, where necessary, kept up to date;
- kept no longer than necessary (storage limitation);
- kept secure, including against loss, damage or unauthorised access (integrity and confidentiality);
- handled in a way A2A can demonstrate and account for (accountability).

4. The personal data we process

Depending on a person's relationship with A2A, the personal data processed may include:

- **Apprentices and learners** – forename and surname, date of birth, sex, email and telephone, unique learner number (from the DfE), apprenticeship standard, start date, gateway date, expected end date and funding type; assessment activity including scheduled dates, assessment materials submitted, recordings of assessments, recorded feedback and results, and internal quality assurance activity.
- **Special-category and statistical data** – information such as age, sex, ethnic origin, and disability or health information relating to reasonable adjustments and special considerations.
- **Criminal offence data** – certificate information for staff and associates who may be allocated apprentices under 18. See section 6.
- **Centre, training provider and employer contacts** – training provider name and coach or tutor contact details; employer name and address and line manager name, role and contact details.
- **Staff and associates** – personnel and contract records, qualifications and occupational competence evidence, continuing professional development, scope of approval, standardisation records and invoices.
- **Applicants for staff and assessor roles** – contact details, CV, qualifications and occupational competence evidence, references, right to work information, and equal opportunities monitoring information where it is provided. A2A may keep an application on file so that the person can be considered for future opportunities.
- **Marketing contacts** – names and contact details held where there is a lawful basis to do so.

5. Our lawful bases

A2A processes personal data where it has a lawful basis under UK GDPR Article 6:

Processing	Lawful basis
Registering apprentices, conducting gateway and assessment, recording results and issuing certificates	Contract; and legal obligation where required by our Conditions of Recognition

Retaining records for internal and external quality assurance and audit	Legal obligation
Sharing information with Ofqual, Skills England or another regulator	Legal obligation, or recognised legitimate interest under Schedule 4 to the Data Protection Act 2018
Managing staff and associates	Contract and legal obligation
Marketing to business contacts	Consent

Consent is used only where it is genuinely the basis for the processing, principally marketing. Withdrawing consent to marketing does not affect the processing A2A carries out to deliver and record assessment, which rests on contract and legal obligation.

6. Special-category and criminal offence data

Some of the data A2A processes is special-category data under UK GDPR Article 9 — in particular ethnic origin, and health or disability information where an apprentice or centre declares it in relation to a reasonable adjustment or special consideration. A2A processes this data only where, in addition to an Article 6 basis, an Article 9 condition applies. A2A relies on the substantial public interest condition for equality of opportunity or treatment, and on explicit consent where the individual supplies health information themselves in support of an adjustment request.

Where consent is withdrawn for health information supplied in support of a reasonable adjustment or special consideration, A2A may be unable to put the adjustment in place or to take the circumstances into account. A2A will explain the effect before acting on a withdrawal of consent.

Criminal offence data and DBS checks

A2A does not carry out Disclosure and Barring Service (DBS) checks and is not a registered body. Where a member of staff or an associate may be allocated apprentices under 18, A2A asks them to hold a current enhanced DBS certificate obtained in their own right, and either to provide the certificate details for verification or to register with the DBS Update Service so that A2A can carry out an online status check.

Whichever route is used, A2A is processing criminal offence data under UK GDPR Article 10 from the point at which it sees a certificate, records certificate details or carries out a status check. A2A processes this data under the safeguarding condition in Part 2, paragraph 18 of Schedule 1 to the Data Protection Act 2018, and holds an Appropriate Policy Document as required by section 42 of that Act. It is set out at Annex B.

A2A does not retain copies of DBS certificates

Once a certificate has been seen and verified, A2A records only the certificate number, the type of check, the date of issue, the date it was seen and by whom, and whether the person is cleared for allocation. The certificate itself is not filed, copied, scanned or forwarded.

Where a certificate is sent to A2A, the copy is deleted once the details have been recorded, including from email inboxes, sent items and deleted items. Where the person is registered with the DBS Update Service, A2A carries out an online status check and records the date and result of that check instead.

A copy is retained only where there is a specific and recorded reason, for example a disclosure requiring a documented risk assessment or an ongoing dispute. Any such copy is held securely by the Director, kept separate from the general personnel file, and destroyed within six months of the decision it supports unless a live matter requires it to be kept longer.

7. How we use personal data

A2A uses personal data to administer and quality-assure assessment and any training it delivers; to register apprentices, conduct gateway and end-point assessment, record results and issue certificates; to meet regulatory and funding

requirements; to manage relationships with centres, providers and employers; to support equality monitoring; and, where there is a lawful basis, for limited marketing.

Automated processing

Some marking is carried out automatically, for example where a knowledge test is marked by the online testing platform. Automated marking does not by itself determine an apprentice's overall grade. Results are reviewed by an assessor, and the grading decision is made by a named assessor in accordance with the applicable assessment plan. Anyone can ask A2A to explain how a result was reached, and can use the Enquiries, Appeals and Complaints Policy (A2A-EAC-POL-001) if they disagree with it.

A2A does not use special-category data in any automated processing or profiling activity, and does not make decisions about individuals by automated means alone.

Assessment recordings

A2A records assessment activity where the applicable assessment plan requires or permits it. A recording may include video and audio, assessment performance and interaction, and information relating to the outcome. Because assessment is delivered remotely, a recording may also incidentally capture other information, such as the surroundings the apprentice is in.

Recordings are used to confirm and review assessment decisions, for internal and external quality assurance, for appeals, complaints and investigations, and for assessor standardisation. Access is restricted to A2A staff involved in quality assurance and compliance, the assessor and internal quality assurer concerned, and regulators or auditors where required.

Where a recording is used for assessor training or standardisation, access is restricted to those taking part in the exercise and the recording is not shared outside that group. Recordings held for this purpose are reviewed periodically and are not kept indefinitely.

8. Sharing personal data

A2A shares personal data only where necessary and lawful — for example with Ofqual and other regulators, the Department for Education, Skills England and the relevant funding body, and with centres, training providers and employers in connection with an apprentice's assessment. A2A discloses information beyond these routes only with appropriate authority and in line with the Conditions of Recognition.

Where A2A confirms that malpractice or qualification fraud has occurred at a training provider, A2A notifies other awarding organisations that may be affected, in the structured format Ofqual has developed for this purpose. This is a requirement placed on A2A by Ofqual and is not optional.

Where a supplier processes personal data on A2A's behalf, a written processor agreement is in place. Personal data is held within the United Kingdom or, where a supplier operates elsewhere, under an appropriate transfer mechanism. Any proposal for a member of staff or an associate to work from outside the United Kingdom must be approved by the Director in advance so that transfer arrangements can be assessed.

9. Systems we use

A2A uses secure, access-controlled systems to store and process personal data. Each supplier publishes its own privacy information, and the location of that information is shown below.

System	Purpose	Supplier privacy information
Microsoft SharePoint, Teams and 365 email	Document storage, correspondence, remote assessment and recording	privacy.microsoft.com/en-GB
Zoom	Remote assessment and recording where a provider requires it	zoom.us/privacy

Proficient (Skilltech Solutions)	Assessment administration, provider and centre records, and storage of assessment evidence	skilltechsolutions.co.uk/privacy-policy
ACE360	Assessment administration, provider and centre records, and storage of assessment evidence	ace360.org/privacy-policy
Highfield Vault	Retained apprentice evidence	highfieldvault.com/privacy-notice
VQ Manager (SkillWise)	Retained apprentice evidence	skillwise.net/vqmanager
ClassMarker	Online knowledge testing	classmarker.com/online-testing/privacy
Sage	Finance and invoicing records	sage.com/en-gb/legal/privacy-and-cookies

Where A2A introduces a further system that will hold personal data, it is assessed before use and this policy is updated at the next review.

Access is granted on a least-privilege basis, reviewed when a person changes role and removed promptly when they leave or their engagement ends. Paper-based records are scanned, uploaded securely and then securely destroyed.

A2A asks apprentices and centres to take care over what they upload, to anonymise information where appropriate, and to remove confidential material that is not required for assessment. Where evidence reaches A2A with third-party information still present, A2A remains the controller of that data once it is in A2A systems and handles it under this policy.

10. Keeping data secure

A2A takes appropriate technical and organisational measures to protect personal data against loss, misuse or unauthorised access. Data is held on password-protected systems and is not shared externally without authority. A2A applies data protection by design and by default, and completes a data protection impact assessment before introducing high-risk new processing.

Multi-factor authentication

Multi-factor authentication is mandatory

Multi-factor authentication must be enabled on every account, email address and system used in connection with A2A work. This is a condition of access, and accounts without it may be suspended. It applies to associates using their own business email or equipment in exactly the same way as it applies to employees.

Multi-factor authentication means signing in with something in addition to a password, normally a code or prompt from an authenticator app. Where a system offers a choice, an authenticator app should be used rather than a text message. If a system used for A2A work does not support multi-factor authentication, this must be raised with the Director rather than the system continuing to be used. A lost device holding an authenticator must be reported immediately so access can be revoked.

Other requirements

- Use strong, unique passwords. Do not reuse an A2A password on another service, and do not share credentials with anyone, including colleagues.
- Lock screens when stepping away, and keep devices encrypted and up to date.
- Do not store apprentice data on personal equipment for longer than is needed to upload it to an A2A system, and delete the local copy once uploaded.
- Do not use personal email, personal cloud storage or unapproved messaging apps for A2A personal data.
- Assess from a private space, do not allow others to overhear, and do not record beyond what the assessment plan requires.

Assessors, internal quality assurers and associates agree to maintain confidentiality as part of their induction and terms of engagement, and a breach of confidentiality is treated as a serious disciplinary matter. All staff who handle personal data undertake data protection training, and A2A retains evidence of this.

11. How long we keep data

Ofqual's Conditions of Recognition require A2A to hold records sufficient to demonstrate compliance, and to keep a log of malpractice and maladministration allegations and investigations. They do not set a retention period. A2A therefore sets its own periods and is able to justify them, taking account of the time within which an appeal, complaint or investigation may arise, the six-year limitation period for contractual claims, retention obligations passed to A2A through training provider contracts, and statutory requirements for financial records.

Record	Retention period
Apprentice assessment records, results and certification decisions	Six years from the date of the result
Gateway evidence, including qualification certificates	Six years from the date of the result
Audio and video recordings of assessment	Six years from the date of the result, so that they remain available for regulatory audit, external quality assurance, appeals and investigations
Appeals, complaints, malpractice and maladministration records	Six years from conclusion of the matter
Provider, employer and centre records, including contact details and signed agreements	For as long as the organisation is working with A2A, and six years afterwards
Staff and associate records	Six years after the engagement ends
Records of applicants who are not appointed or approved	Six years from the end of the recruitment or approval process, or sooner if the applicant asks A2A to remove their information, in which case it is removed immediately
DBS record of check	Duration of the engagement and six years afterwards
Financial and invoicing records	Six years from the end of the accounting period
Marketing contact data	Until the person opts out

A record held for longer than the period above is retained only for a stated reason, recorded at the time. Where a training provider contract imposes a longer period than the one shown, the contractual period applies for the records it covers.

A2A reviews its data holdings periodically to confirm that records are still required, that the periods above are being applied, and to identify records for disposal. Digital records are securely deleted, and where a record is held in a supplier system, deletion is confirmed with the supplier. Any remaining paper records are destroyed by cross-cut shredding or confidential waste disposal.

12. Your rights

Individuals have rights over their personal data under the UK GDPR, including the right to be informed; to access their data (a subject access request); to rectification; to erasure; to restrict or object to processing; to data portability; and to be told about any automated decision-making and have the logic behind it explained, where these apply. There is no charge for exercising these rights, and A2A will respond within one month. Where a request is complex, or where several requests are made, A2A may extend this by up to two further months and will explain why. A2A carries out a reasonable and proportionate search in response to a request.

To protect your information, A2A will ask you to verify your identity before responding to a rights request. Where a request is made on your behalf, A2A will ask that person to show they have your authority to act. The response period runs from the point at which A2A has what it needs to identify you and locate your data.

Where you agree, A2A will try to deal with a request informally — for example by providing the specific information you need directly — rather than by carrying out a full search. Where A2A cannot action a request, it will explain why.

Where A2A relies on consent, it can be withdrawn at any time by contacting info@a2aqualifications.co.uk.

Some information is exempt from disclosure. Exam and assessment scripts are exempt under the Data Protection Act 2018, and results may be released on a modified timescale. A2A may also withhold information where releasing it would undermine the validity or integrity of assessment, or A2A's duties under Ofqual's Conditions of Recognition. Where an exemption is applied to any part of a request, A2A will say so and explain which exemption is relied on.

13. Personal data breaches

A personal data breach is any incident that leads to personal data being lost, destroyed, altered, disclosed or accessed without authorisation. Sending an email to the wrong recipient, losing a laptop and leaving a session recording accessible are all examples.

Anyone who thinks a breach may have happened must report it to the Director immediately, and in any event the same day, without waiting to be certain and without attempting to resolve it first. Where a breach is likely to result in a risk to people's rights and freedoms, A2A will notify the ICO without undue delay and, where required, within 72 hours of becoming aware of it, and will inform affected individuals where the risk is high.

All breaches and suspected breaches are recorded, investigated and reviewed, whether or not they are reportable. Breaches are handled alongside A2A's complaints and malpractice arrangements as appropriate. Where a breach arises from a failure to follow this policy it may be dealt with under A2A's disciplinary arrangements or, for associates, under the terms of engagement.

14. Marketing

A2A holds names and contact details for marketing only where it has a lawful basis, and asks people to opt in where required. Anyone can opt out at any time and A2A acts on that promptly. A2A displays the logos or testimonials of organisations it works with only with their permission.

15. Data protection complaints

Anyone who is unhappy with how A2A has handled their personal data can complain to A2A directly. There is no set way to do this. You can:

- email info@a2aqualifications.co.uk;
- write to A2A Qualifications Limited; or
- complete the complaint form at Annex A and send it to A2A by email or post.

A complaint does not have to use the form, and does not have to use any particular wording. A2A will treat any communication as a data protection complaint where that is clearly what it is.

A2A will acknowledge a complaint within 30 days of receiving it, investigate it without undue delay, keep the complainant updated on progress, and inform them of the outcome. Where A2A is not certain of the identity of the person complaining, or where a complaint is made on behalf of someone else, A2A may ask for proof of identity or written authority before proceeding.

Data protection complaints are handled under the Enquiries, Appeals and Complaints Policy (A2A-EAC-POL-001) and are recorded on A2A's complaints log.

Complain to A2A first

Following changes made by the Data (Use and Access) Act 2025 which took effect on 19 June 2026, a data protection complaint should be raised with A2A before it is taken to the Information Commissioner. Individuals retain the right to approach the Commissioner if they remain dissatisfied: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF; helpline 0303 123 1113; ico.org.uk.

16. Roles and responsibilities

- **Director / policy owner** – owns this policy, makes it available, and ensures it forms part of staff training.
- **Data protection lead** – advises on lawful bases, special-category and criminal offence processing, handles rights requests, complaints and breaches, and confirms processor terms.
- **Staff, assessors, IQAs and associates** – follow this policy, complete data protection training, maintain multi-factor authentication on all A2A systems, and maintain confidentiality.

17. Related documents

- Reasonable Adjustments and Special Considerations Policy (A2A-RAS-POL-004)
- Malpractice, Maladministration and Sanctions Policy (A2A-MMS-POL-002)
- Conflict of Interest and Whistleblowing Policy (A2A-CIW-POL-003)
- Enquiries, Appeals and Complaints Policy (A2A-EAC-POL-001)
- Artificial Intelligence (AI) in Assessment Policy (A2A-AI-POL-005)
- Staff and Associates Handbook (A2A-HR-HB-001)
- Expected Behaviour and Respect for Staff Policy (A2A-CON-POL-010)

18. Version history

Version	Date	Owner	Summary of change
1.0	10 June 2026	Director	Rebuilt from A2A Training Data Protection Policy V4 (6 October 2024) into A2A Qualifications house style. Modernised to UK GDPR / Data Protection Act 2018: added data controller and ICO detail, lawful bases, special-category (Article 9) handling, data subject rights, breach notification, data sharing and complaints to the ICO. Removed the blanket disclaimer of responsibility for data loss; updated identity, contacts and systems.
1.1	August 2026	Director	Updated for the Data (Use and Access) Act 2025. Section 15 rewritten for the statutory complaints duty in force from 19 June 2026, with a complaint form added at Annex A. Criminal offence data and DBS handling added at section 6, confirming that A2A does not retain copies of DBS certificates. Appropriate Policy Document added at Annex B. Mandatory multi-factor authentication added at section 10. Lawful bases set out as a table. Retention set out as a table with the basis for each period stated, correcting the previous implication that periods derive from Ofqual requirements. Systems list completed. Exemption wording at section 12 clarified.

Annex A: Data protection complaint form

Use this form if you are unhappy with how A2A Qualifications Limited has handled your personal data. You do not have to use it — an email or letter is equally valid. Send the completed form to info@a2aqualifications.co.uk or by post to A2A Qualifications Limited. A2A will acknowledge it within 30 days of receipt.

Your details	
Name	
Email address	
Telephone (optional)	
Your relationship to A2A (apprentice, provider, employer, staff, associate, other)	

Your complaint	
What happened, and when	
Which of your personal data is involved	
Have you raised this with us before? If so, when and with whom	
What outcome are you looking for	

Signature	
Date	

What A2A does with this form

A2A uses the information given to investigate and respond to the complaint, and to keep a record of complaints received. Complaint records are kept for six years. If you are not satisfied with A2A's response you can raise the matter with the Information Commissioner at ico.org.uk.

Annex B: Appropriate Policy Document

This annex is the Appropriate Policy Document required by section 42 of the Data Protection Act 2018 where A2A Qualifications Limited processes special-category or criminal offence data under a condition in Schedule 1 to that Act. The Information Commissioner accepts that a single document covering all such processing is sufficient, and this annex serves that purpose. It is reviewed alongside this policy and retained for six months after the processing it covers has ceased.

It applies to information held in any form, including email, documents, photographs, and audio and video recordings of assessment. A2A Qualifications Limited is registered with the Information Commissioner's Office under reference ZB263774.

B1. Data covered and conditions relied on

Data	Purpose	Schedule 1 condition
Health information supporting a reasonable adjustment or special consideration	Assessing and putting in place an adjustment so an apprentice can access assessment fairly	Part 2, paragraph 8: equality of opportunity or treatment. Explicit consent is also obtained where the individual supplies the information themselves
Ethnicity, religion and other equality monitoring data	Monitoring and reporting on equality of access and outcomes across assessment	Part 2, paragraph 8: equality of opportunity or treatment
DBS certificate details and Update Service status checks for staff and associates	Confirming suitability to be allocated apprentices under 18. Certificates are obtained by the individual, not by A2A	Part 2, paragraph 18: safeguarding of children and of individuals at risk
Information arising from malpractice and maladministration allegations, including allegations of dishonesty	Investigating and determining allegations as required by our Conditions of Recognition, and reporting where required	Part 2, paragraph 12: regulatory requirements relating to unlawful acts, dishonesty, malpractice or other seriously improper conduct
Information processed in connection with a legal claim	Obtaining legal advice and establishing, exercising or defending legal rights, including prospective proceedings	Part 3, paragraph 33: legal claims

B2. How we comply with the principles

- Lawfulness, fairness and transparency: the processing is described in this policy and in the privacy information given at the point of collection.
- Purpose limitation: this data is used only for the purpose it was collected for and is not reused for another purpose.
- Data minimisation: A2A asks for the minimum needed. For adjustments, A2A asks what the person needs, not for a full medical history. For DBS, A2A records the certificate details and does not retain the certificate.
- Accuracy: records are checked at the point of entry and corrected promptly if an error is identified.
- Storage limitation: retention is set out at B3 and applied through scheduled review.
- Integrity and confidentiality: access is restricted to the Director and, for adjustment data, the assessor delivering the adjustment. Multi-factor authentication is mandatory on all systems. Data is held on password-protected systems and is not held on paper.
- Accountability: this document, the record of processing activities and the training record together evidence how A2A meets these requirements.

B3. Retention and erasure

Data	Retention
Adjustment and special consideration records	Six years from the date of the result, in line with the table at section 11
Equality monitoring data	Aggregated for reporting, with the identifiable source data deleted after the reporting year
DBS record of check	Duration of the engagement and six years afterwards
DBS certificate copy, where exceptionally retained	Six months from the decision it supports, unless a live matter requires longer. Reason recorded at the time

Erasure is carried out securely. Where data is held in a third-party system, deletion is confirmed with the supplier.

B4. Review

This Appropriate Policy Document is reviewed annually with the Data Protection and Privacy Policy, and whenever a new category of special-category or criminal offence data is introduced. Owner and approver: Director.