LONDON PROFESSIONAL ACADEMY (LPA)

Title:	ELECTRONIC SIGNATURES POLICY
Policy Number	P0091
Approved Date:	Sep, 2022
Approved by:	Academic Board London Professional Academy
Review Date:	Sep, 2023
Review Date:	Sep, 2024
Review Date:	Sep, 2025
Next Review Date:	Sep, 2026

1. Purpose

This policy sets out the framework for the lawful, secure, and reliable use of electronic signatures (e-signatures) within London Professional Academy (the "Academy"). It applies to internal approvals, learner agreements, enrolment forms, assessment declarations, and other official documents.

2. Scope

This policy applies to:

- All staff, contractors, and authorised representatives of the Academy.

- Learners, applicants, and third parties who are required to sign Academy documents electronically.

3. Legal Basis

The Academy recognises e-signatures as legally valid under:

- The Electronic Communications Act 2000 (UK)

- The UK eIDAS Regulation (retained EU Regulation No 910/2014)

No contract or signature shall be denied legal effect or admissibility solely because it is in electronic form.

4. Definition of Electronic Signatures

For the purposes of this policy:

- Simple Electronic Signature (SES) – e.g., typed name, ticked box, scanned image of a wet signature.

- Advanced Electronic Signature (AES) – linked uniquely to the signatory, capable of identifying them, and created using a secure signature creation device.

- Qualified Electronic Signature (QES) – AES based on a qualified certificate and created by a qualified signature creation device (rarely required for Academy daily operations).

The Academy will use SES for most routine documents and AES where higher assurance is needed (e.g., financial agreements).

5. Permitted Use of E-Signatures

E-signatures may be used for:

- Enrolment,registration and admission forms

- Learner terms and conditions

- Payment plans and direct debit mandates

- Assessment and plagiarism declarations for Assignments and other required learning material.

- Consent forms (e.g., for work placements, data processing)

- Internal approval documents (e.g., expense claims, leave requests)

Exclusions (paper signatures still required):

- Wills, trusts, or lasting powers of attorney

- Court orders or statutory declarations (unless otherwise permitted by law)

- Certain documents requiring a wet signature under specific regulatory rules (e.g., some funding body declarations – refer to compliance).

6. Acceptable Methods

The Academy approves the following e-signature solutions:

- Adobe Sign

- Microsoft Forms (with recorded email confirmation)

- Secure PDF with form fields (where signature log is retained)

Staff must ensure the chosen method:

- Captures the signatory's name and timestamp.

- Provides an audit trail (IP address, email, date/time) where possible.

- No shared or generic email accounts shall be used for signing official documents.

7. Identity Assurance

The Academy requires reasonable identity verification for e-signatures:

- For learner documents: signature email must match the personal email/student record.

- For high-risk agreements: additional verification (e.g., ID check, video call, or multi-factor authentication) is required before sending.

- Staff must not sign on behalf of another person unless they have explicit legal authority (e.g., power of attorney).

8. Consent and Opt-Out

- By submitting an e-signed document, the signatory consents to the use of e-signatures.

- Individuals may request to sign a wet-ink paper version instead. The Academy will accommodate such requests without penalty, though processing may take longer.

- Any refusal to use e-signatures must be documented by the Academy's compliance team.

9. Record Retention and Audit

- Signed electronic documents shall be retained for the same period as paper records (minimum 6 years for learner records, longer where funding or legal conditions apply).

- Audit logs (if supported by the platform) must be retained alongside the signed document.

- The Academy will periodically review e-signature processes for security and legal compliance.

10. Security and Misuse

- E-signature platform access shall be protected by strong passwords and, where possible, multi-factor authentication (MFA).

- Staff must not tamper with an e-signed document after signing.

- Any suspected forgery, coercion, or unauthorised use of another's e-signature must be reported immediately to the Director for compliance.

11. Policy Breach

Breaches of this policy may lead to disciplinary action (for staff) or exclusion/contract termination (for learners or third parties). Unauthorised e-signatures may be declared void.

12. Responsibilities

- IT & Systems Manager – Maintains approved e-signature platforms and security.

- Compliance Officer – Oversees legal alignment and handles opt-out/waiver requests.

- All signatories – Ensure they understand the document before signing and keep their signing credentials secure.

13. Review

This policy will be reviewed annually and updated for changes in UK law, technology, or Academy operations.