

Data Protection and Information Security Policy

Document reference	UKSEQ-POL-011
Policy area	Compliance
Version	0.1 — Draft
Status	In development — not approved for operational use
Policy owner	UKSEQ Quality & Compliance Lead (proposed)
Approval authority	UKSEQ Board (proposed)
Effective date	To be confirmed upon approval
Review frequency	Annually and following material change
Next review	12 months after approval

1. Purpose and scope

This policy establishes the proposed UKSEQ approach to data protection and information security. It applies to UKSEQ directors, employees, contractors, centres and learners as relevant to their roles. It will take effect only when formally approved and implemented. UKSEQ is not currently recognised by Ofqual or Qualifications Wales and does not currently award regulated qualifications.

2. Responsibilities

The Board is accountable for approving the policy and ensuring sufficient resources and independent oversight. The designated Quality & Compliance Lead is responsible for implementation, monitoring and escalation. Centres and authorised personnel must comply with applicable requirements, cooperate with reviews and maintain accurate records. Specific appointments and delegated authorities must be confirmed before the policy takes effect.

3. Governance

UKSEQ will comply with applicable UK data protection law, including the UK GDPR and Data Protection Act 2018, and establish clear controller/processor roles with centres and suppliers.

4. Lawful processing

Each processing activity must have a documented purpose, lawful basis, privacy information, retention period and appropriate security controls. Special-category data requires an additional lawful condition.

5. Data minimisation and rights

Collect only necessary data and provide processes for access, rectification, erasure where applicable, restriction, objection and other relevant rights within statutory timeframes.

6. Access control

Use least-privilege, role-based permissions, MFA for privileged access, strong authentication, separation of duties and prompt removal of access when roles change.

7. Security and suppliers

Apply encryption, patching, logging, backup testing, vulnerability management, supplier due diligence, contractual safeguards and documented international transfer assessments where required.

8. Incidents and breaches

Personnel must report suspected breaches immediately. UKSEQ will assess risk, contain the incident, record decisions and notify the ICO within 72 hours where legally required, and affected people where the legal threshold is met.

9. Retention and disposal

Learner, assessment and certification records must follow an approved retention schedule reflecting legal, regulatory and verification requirements. Disposal must be secure and auditable.

10. Oversight

UKSEQ will maintain records of processing, DPIAs where required, training, policy review and independent assurance proportionate to risk.

11. Monitoring, records and review

Compliance will be monitored through management review, sampling, incident analysis and internal audit as appropriate. Records of decisions, exceptions, approvals and corrective actions must be maintained in approved secure systems. This policy will be reviewed annually, and sooner following relevant legal or regulatory change, material incident or identified weakness.

12. Related documents

This policy should be read alongside the UKSEQ policy suite, applicable qualification specifications, approved centre agreements and relevant statutory or regulatory requirements. In any conflict, applicable law and binding regulatory conditions take precedence.

Document control and approval

Prepared for consultation and Board review. Before issue, UKSEQ must confirm named accountable officers, contact routes, delegated decision rights, service standards, implementation evidence and any necessary regulatory cross-references.

Approved by	Pending
Approval date	Pending
Next scheduled review	12 months after approval