

HiQual UK

DATA PROTECTION & UK GDPR POLICY

HQUK-POL-DP-001

Document Control Item	Details
Organisation	HiQual UK
Policy Title	Data Protection & UK GDPR Policy
Policy Reference	HQUK-POL-DP-001
Version	1.0
Policy Status	Approved
Effective Date	1 June 2026
Next Review Date	1 June 2027
Policy Owner	Sarah Williams, Head of Quality Assurance
Approved By	HiQual UK Academic and Standards Committee
Review Cycle	Annual, or earlier where legal, regulatory, operational or organisational changes require review
Classification	Public Policy
Applies To	Learners, Approved Centres, Assessors, Internal Quality Assurers, Tutors, HiQual UK Personnel, Contractors and Relevant Stakeholders

Framework for lawful, fair, transparent and secure processing of personal data

1. Purpose

HiQual UK is committed to protecting the privacy, confidentiality and rights of individuals whose personal data it processes.

This policy establishes the principles, responsibilities and controls HiQual UK will use to comply with applicable UK data protection law, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and other applicable data protection and privacy requirements.

The policy is designed to support accountability, appropriate security, lawful processing and effective management of individual rights.

2. Scope

This policy applies to personal data processed by or on behalf of HiQual UK in connection with qualifications, learners, centres, assessment, certification, quality assurance, governance, administration, personnel, suppliers, communications and other organisational activities.

It applies to HiQual UK personnel, Approved Centres and relevant third parties where their activities involve personal data processed on behalf of or in connection with HiQual UK.

3. Legal and Regulatory Framework

HiQual UK will maintain arrangements appropriate to the legal framework applicable to its processing activities. This includes the UK GDPR and DPA 2018 and, where relevant, privacy and electronic communications requirements and other applicable legislation.

Because UK data protection requirements and regulatory guidance may change, this policy will be reviewed when material legislative or regulatory changes occur. Current ICO guidance should be considered when applying this policy.

4. Data Protection Principles

HiQual UK will apply the UK GDPR principles to personal data processing. Personal data will be:

4.1 Lawfulness, Fairness and Transparency

Processed lawfully, fairly and transparently in relation to the individual.

4.2 Purpose Limitation

Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes.

4.3 Data Minimisation

Adequate, relevant and limited to what is necessary for the purposes for which it is processed.

4.4 Accuracy

Accurate and, where necessary, kept up to date, with reasonable steps taken to correct inaccurate personal data.

4.5 Storage Limitation

Kept in an identifiable form for no longer than necessary, subject to legitimate retention requirements.

4.6 Integrity and Confidentiality

Processed using appropriate security measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage.

4.7 Accountability

HiQual UK will take responsibility for compliance and maintain appropriate measures and records to demonstrate compliance.

5. Key Definitions

Personal data means information relating to an identified or identifiable living individual.

Processing means an operation or set of operations performed on personal data, including collection, recording, organisation, storage, alteration, retrieval, consultation, use, disclosure or deletion.

Data controller means the organisation that determines the purposes and means of processing personal data.

Data processor means a person or organisation that processes personal data on behalf of a controller.

Personal data breach means a security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

6. Data Controller and Processor Responsibilities

HiQual UK will determine and document its role as controller, processor or joint controller for relevant processing activities.

Where HiQual UK appoints a processor, appropriate contractual arrangements and due diligence will be used to ensure the processor provides sufficient guarantees for compliance and security.

Approved Centres and other organisations must comply with relevant contractual data protection requirements when processing HiQual UK-related personal data.

7. Lawful Bases for Processing

HiQual UK will identify and document an appropriate lawful basis before processing personal data. Depending on the purpose, lawful bases may include consent, contract, legal obligation, vital interests, public task or legitimate interests.

Consent will not be treated as the default basis where another lawful basis is more appropriate.

Where legitimate interests are relied upon, HiQual UK will consider and document the relevant balancing and necessity considerations.

8. Special Category Data

HiQual UK recognises that special category data requires additional protection. Examples include data concerning health, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic data, biometric data used for unique identification, sex life and sexual orientation.

Where special category data is processed, HiQual UK will identify both an Article 6 lawful basis and an applicable Article 9 condition and any additional requirements under UK law.

Where required, HiQual UK will maintain an Appropriate Policy Document and apply additional safeguards, retention controls and security measures.

9. Criminal Offence Data

Where HiQual UK processes personal data relating to criminal convictions, offences or allegations, it will apply the additional requirements applicable to such data under the UK GDPR and DPA 2018.

Such processing will be limited to necessary and justified purposes and subject to appropriate safeguards and documentation.

10. Privacy Information and Transparency

HiQual UK will provide clear privacy information to individuals explaining, as appropriate, what personal data is collected, purposes of processing, lawful bases, recipients, retention, rights and other required information.

Privacy information will be reviewed when processing activities materially change.

11. Individual Rights

HiQual UK will respect applicable data subject rights, including:

11.1 Rights

Right to be informed.

Right of access.

Right to rectification.

Right to erasure, where applicable.

Right to restrict processing, where applicable.

Right to data portability, where applicable.

Right to object, where applicable.

Rights relating to automated decision-making and profiling where applicable.

12. Handling Rights Requests

Requests will be handled through a documented process designed to verify identity where necessary, locate relevant information, assess exemptions or restrictions and respond within applicable statutory timescales.

Requests will be logged and escalated where complexity, exemptions, third-party information, special category data or other factors require specialist consideration.

13. Children and Learners

Where HiQual UK processes personal data relating to children or young learners, additional care will be taken to ensure that privacy information and processing arrangements are appropriate to their age and understanding.

Where consent is the lawful basis for an online service offered directly to a child, HiQual UK will apply the applicable requirements for valid consent.

14. Data Protection by Design and Default

Data protection will be considered from the beginning of new or materially changed projects, systems, qualifications, assessment processes and services.

HiQual UK will seek to minimise personal data collection, limit access, use appropriate security, avoid unnecessary retention and build privacy safeguards into relevant processes.

15. Data Protection Impact Assessments

HiQual UK will consider whether a Data Protection Impact Assessment (DPIA) is required for processing likely to result in a high risk to individuals.

DPIAs will assess necessity, proportionality, risks to individuals and measures to mitigate those risks.

Where a high residual risk cannot be adequately mitigated, HiQual UK will consider whether prior consultation with the ICO is required.

16. Records of Processing Activities

HiQual UK will maintain appropriate records of processing activities where required. Records may include purposes, categories of individuals and data, recipients, retention periods, security measures and relevant international transfers.

Records will be reviewed and updated when processing changes.

17. Data Security

HiQual UK will implement appropriate technical and organisational measures proportionate to the risks associated with its processing.

Security measures may include access controls, authentication, encryption where appropriate, secure storage, backups, secure transfer, logging, staff training, confidentiality arrangements and incident response procedures.

18. Access Control and Confidentiality

Access to personal data will be restricted to persons who require it for legitimate duties.

Users must not access, copy, disclose or use personal data beyond their authorised responsibilities.

Confidentiality obligations will continue after a person's role or relationship with HiQual UK ends.

19. Data Retention and Disposal

HiQual UK will retain personal data only for as long as necessary for the purpose for which it is processed or where retention is required or justified by law, contractual obligations, qualification records, governance or legitimate business requirements.

Retention periods will be documented in a retention schedule or relevant procedure.

Personal data will be securely deleted, destroyed or anonymised when it is no longer required, subject to legal holds or other legitimate retention requirements.

20. Data Sharing

HiQual UK will only share personal data where there is a lawful basis and the sharing is necessary and proportionate.

Sharing may occur with Approved Centres, assessors, quality assurance personnel, certification partners, service providers, professional advisers, regulators or public authorities where appropriate.

Before routine or significant sharing arrangements are implemented, HiQual UK will consider purpose, lawful basis, necessity, security, confidentiality and contractual requirements.

21. International Data Transfers

Where personal data is transferred outside the UK or otherwise made available internationally, HiQual UK will ensure that the applicable UK GDPR transfer requirements and safeguards are satisfied.

Appropriate transfer mechanisms, adequacy arrangements, contractual safeguards or other lawful measures will be considered as applicable.

22. Third-Party Processors

HiQual UK will undertake proportionate due diligence before appointing processors and will maintain written contracts containing appropriate data protection obligations.

Processors will only process personal data on documented instructions and must apply appropriate confidentiality and security measures.

HiQual UK will monitor processor arrangements proportionately and review them where risks or processing activities change.

23. Personal Data Breaches

All personnel and relevant centres must report suspected personal data breaches promptly through the designated internal route.

A breach may include accidental disclosure, loss, theft, unauthorised access, alteration, destruction or other compromise of personal data.

HiQual UK will assess breaches promptly, contain and mitigate risks, document the incident and determine whether notification to the ICO or affected individuals is required.

24. ICO Breach Notification

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, HiQual UK will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of the breach, where notification is required.

Where a breach is likely to result in a high risk to individuals, HiQual UK will consider whether affected individuals must also be informed without undue delay.

All breaches will be recorded as required, including breaches that do not meet the threshold for notification.

25. Complaints and Concerns

Individuals may raise concerns about HiQual UK's handling of personal data through the relevant contact route and complaints process.

Where appropriate, individuals may also complain directly to the ICO. HiQual UK will cooperate with lawful regulatory enquiries and investigations.

26. Data Protection Officer / Responsible Person

HiQual UK will determine whether it is legally required to appoint a Data Protection Officer (DPO). Where a DPO is required, the DPO will have appropriate independence, resources and access to senior management.

Where a formal DPO is not required, HiQual UK will designate an appropriate data protection contact or responsible person to coordinate compliance activities.

27. Staff and Centre Training

Relevant personnel will receive appropriate data protection awareness and training.

Training will cover confidentiality, secure handling, phishing and social engineering risks, breach reporting, individual rights and role-specific responsibilities.

Approved Centres are expected to ensure personnel involved in HiQual UK activities understand relevant data protection obligations.

28. Monitoring and Audit

HiQual UK will monitor its data protection arrangements through appropriate reviews, audits, incident analysis, rights-request monitoring, processor reviews and other assurance activities.

Significant findings will be reported to the appropriate governance body and corrective action will be tracked to completion.

29. Data Protection and Equality Information

Where HiQual UK processes equality, diversity, disability, health or other sensitive information, it will apply the additional safeguards required for special category data and ensure that collection and use are necessary and proportionate.

30. Automated Decision-Making and Profiling

Where HiQual UK uses automated decision-making or profiling that falls within applicable UK GDPR requirements, it will assess the relevant legal requirements and safeguards, including applicable rights and the need for meaningful human involvement.

HiQual UK will not introduce solely automated decisions with significant effects without appropriate legal assessment and safeguards.

31. Governance and Accountability

The Governing Board has overall responsibility for ensuring that HiQual UK maintains appropriate arrangements for data protection and information governance.

The Academic and Standards Committee will oversee significant data protection matters where they affect learners, qualification integrity, assessment, certification or organisational risk.

The Policy Owner or designated data protection lead will coordinate implementation, maintain relevant records, support risk assessments and escalate significant concerns.

32. Policy Breaches

Failure to comply with this policy may result in corrective action, additional training, restriction of access, disciplinary action, contractual action or other appropriate measures.

Where a breach may involve unlawful processing, fraud, safeguarding concerns or other serious misconduct, HiQual UK may refer the matter to the appropriate authority.

33. Policy Exceptions

Any exception to this policy must be justified, documented and approved by an appropriately authorised person or governance body.

No exception may be used to avoid a legal obligation, conceal a breach or expose individuals to unnecessary data protection risks.

34. Policy Review

This policy will be reviewed at least annually and sooner where required by changes in UK data protection law, ICO guidance, the Data (Use and Access) Act 2025 or other applicable requirements, organisational changes, security incidents, audits or lessons learned.

The Policy Owner will recommend amendments to the appropriate governance authority for approval.

35. Related Policies and Procedures

This policy should be read alongside:

- Privacy Notice / Learner Privacy Notice
- Staff Privacy Notice
- Information Security Policy
- Data Breach / Personal Data Breach Procedure
- Records Management and Retention Policy
- Data Protection Impact Assessment Procedure
- Data Subject Rights Procedure
- Data Sharing and Information Disclosure Procedure
- Supplier and Data Processor Management Procedure
- Equality, Diversity & Inclusion Policy
- Malpractice and Maladministration Policy
- Complaints Policy
- Academic Governance Policy
- Quality Assurance Policy
- Whistleblowing Policy

36. Document Control

Document Control Item	Details
Organisation	HiQual UK
Policy Title	Data Protection & UK GDPR Policy
Policy Reference	HQUK-POL-DP-001
Version	1.0
Effective Date	1 June 2026
Policy Owner	Sarah Williams, Head of Quality Assurance
Approval Authority	Academic and Standards Committee
Approved Status	Approved
Review Date	1 June 2027
Review Frequency	Annual
Classification	Public Policy
Applies To	Learners, Approved Centres, Assessors, Internal Quality Assurers, Tutors, HiQual UK Personnel, Contractors and Relevant Stakeholders

37. Version Control

Version	Date	Description of Change	Author	Approval
1.0	1 June 2026	Initial publication of HiQual UK Data Protection & UK GDPR Policy	Sarah Williams, Head of Quality Assurance	Academic and Standards Committee

38. Policy Statement

HiQual UK is committed to protecting personal data and respecting the privacy and rights of individuals. Personal data will be processed lawfully, fairly, transparently, securely and only to the extent necessary for legitimate purposes.

HiQual UK will maintain appropriate governance, technical and organisational measures to demonstrate compliance with applicable UK data protection law, manage risks, respond to individual rights and address personal data breaches.

This policy is intended to provide a practical governance framework and must be applied together with relevant procedures, privacy notices, contracts and current regulatory guidance.

END OF POLICY