QAHE Limited
Data Protection and Privacy Policy

Prepared by: Chief Governance & Transformation Officer

Prepared for: Board of Directors

Date: May 2026

Issue: 1

Version Control

Document Information	
VO1	Original draft of the Data Protection Policy

Document Approval		
Board	**Approval**	**Viewed / Comments Date**
Chief Governance & Transformation Officer	Approved	May 2026
		Approved

Revision History			
Version	**Issue Date**	**Author**	**Description of Change**
VO1	May 2026	Chief Governance & Transformation Officer	Policy based on the QA Group Data Protection Policy. Policy amended for the structure of QAHE and for approval by the Board of Directors.

© 2026 QAHE Limited. All rights reserved.

Contents

© 2026 QAHE Limited. All rights reserved.

1. Introduction

QAHE Limited ("QAHE") is a part of the QA Group. As part of a wider group structure, we operate a comprehensive framework of policies designed to safeguard our organisations and uphold the highest standards of integrity, this is our Data Protection Framework.

As part of QA Group our operations are ISO27001 certified, CyberEssentials Plus certified, and take information security and data privacy very seriously, valuing the personal and commercial data with which we are entrusted.

QAHE must comply with the requirements of applicable data protection legislation including UK data protection legislation, principally the UK General Data Protection Regulation, (referred to as 'UK GDPR') as amended and supported by the Data Protection Act 2018 (hereafter referred to as 'the Act'). These define personal data as "any information related to an identified or identifiable natural person ('data subject').

QAHE is registered with the Information Commissioner's Office (ICO), reflecting its position as a Data Controller. The status of QAHE as a Data Controller or Data Processor is defined in contract documents, including data sharing or data processing agreements.

2. Objective

This Data Protection and Privacy Policy, in conjunction with supporting information security policies and controls, demonstrate commitment and support by QAHE's Executive Team to the secure management of personal data in compliance with data protection legislation.

This Policy and the supporting measures promote and demand consistent standards and practices for processing personal data to allow QAHE to meet its legal obligations and strategic objectives.

3. Scope

This Policy applies to all staff and others working for or on behalf of QAHE whether in the UK or overseas and includes; directors, secondees, any third-party representatives, agency workers, volunteers, interns, agents, and sponsors. Staff employed by QAHE must ensure that this policy is communicated to any organisation that they work with who may have access to the personal data where QAHE is data controller.

The act of "processing" personal data is a broad set of activities that includes "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Personal data of extra sensitivity has even greater conditions for processing. Known under the UK GDPR as 'Special Category Data', this is personal data revealing or concerned with:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Health
- Sex life or sexual orientation.

© 2026 QAHE Limited. All rights reserved.

Processes or systems processing this data are reviewed prior to data capture to confirm processing is valid and secure.

4. Policy Statement

The lawful and correct processing of personal data is vital to the successful operation and reputation of QAHE, and for maintaining the trust of our employees, students, and other stakeholders. QAHE is committed to protecting the rights and freedoms of individuals in accordance with the provisions of applicable data protection legislation. In order to achieve this, QAHE has implemented and maintains a framework, which ensures that personal data is handled appropriately and consistently.

QAHE will comply with the following data protection principles when processing personal data:

- We will process personal data lawfully, fairly and in a transparent manner
- We will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes
- We will only process the personal data that is adequate, relevant and necessary for the relevant purposes
- We will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay
- We will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed
- We will take appropriate technical and organisational measures to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

As such, QAHE implements appropriate and effective measures to ensure that:

- Personal data is:
  - Obtained and processed lawfully and fairly
  - Collected only where necessary for legal, regulatory and business purposes and are processed in accordance with applicable data protection legislation
  - Accurate when collected and, where necessary, are kept up to date
  - Only retained for as long as is necessary for the purposes of the processing, subject to other legal and regulatory requirements
  - Protected against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data by implementing appropriate technical and organisational measures
  - Not processed for purposes that are incompatible with the original purposes for which they were obtained
  - Not unnecessarily disclosed to third parties
  - Not transferred outside the European Economic Area (EEA) or the United States unless an adequate level of protection for the rights and freedoms of the data subjects, in relation to processing personal data, can be assured.
- Data subjects are:
  - Provided with clear information as to the purposes for which their personal data are collected and processed; and
  - Informed of their rights in relation to the processing of their personal data under applicable data protection legislation, and that these rights are respected.
- Appropriate internal controls, including policies, standards, processes and guidance, are implemented and maintained to encourage consistent approaches to processing personal data across QAHE.

© 2026 QAHE Limited. All rights reserved.

- Roles and responsibilities in relation to processing personal data are clearly defined, documented and effectively communicated.
- Appropriate data protection training and awareness is provided to all employees, and contract hires to assist them with understanding and implementing their responsibilities in relation to processing personal data.
- Suppliers processing personal data on behalf of QAHE are subject to a due diligence process, contractual controls and, where appropriate, ongoing assurance checks to ensure that they implement and maintain appropriate technical and organisational security measures to protect personal data belonging to QA and its clients.
- A Data Protection Officer (DPO) is appointed with oversight of QAHE's data compliance processes, in conjunction with the Head of Legal.
- QAHE is registered as a Data Controller with the ICO under registration number ZA481225.

5. Basis for Processing

In relation to any processing activity we will, as applicable, before the processing starts for the first time, and then regularly while it continues:

- Review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
  - That the data subject has consented to the processing
  - That the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
  - That the processing is necessary for compliance with a legal obligation to which the Company is subject
  - That the processing is necessary for the protection of the vital interests of the data subject or another natural person
  - That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority, or
  - That the processing is necessary for the purposes of legitimate interests of the Company or a third party (including a regulator), except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).
- Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.
- Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
- Where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it.
- Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

6. Roles and Responsibilities

QAHE's suppliers that process personal data on behalf of QAHE are required to comply with this Policy and other terms and conditions set in place as part of any contract, including but not limited to data sharing/processing agreements.

The DPO (as supported by the Head of Legal) acts as a point of reference for data protection within QAHE and sets and oversees the overall data protection strategy. The DPO periodically

© 2026 QAHE Limited. All rights reserved.

reviews the planning, implementation, effectiveness and progress of QAHE's data protection controls and initiatives, reporting to QAHE's Executive Board as required. The DPO acts as an escalation point for material data protection risks or incidents, liaising with the ICO where appropriate.

More detailed responsibilities of key roles are described in the QAHE Information Security Policy and the QAHE Information Security Management System (ISMS) Policy.

7. International Transfers

QAHE may transfer, store, and process personal information outside the UK and/or the EEA, including but not limited to international organisations. Transfers of personal information are legally permitted, amongst other mechanisms, under International Data Transfer Agreements (IDTAs) for controllers, and where relevant for processors. When we transfer, store, or process personal data, we do so in accordance with our privacy notices and applicable law, including the implementation of appropriate and adequate safeguards in seeking to ensure that personal data is transferred to an adequate level of protection.

For information about transfers please contact privacy@qa.com.

8. Storage and retention of personal information

Personal information (and sensitive personal information) is kept securely in accordance with QAHE's Information Security Policy.

Personal information (and sensitive personal information) is not retained for any longer than necessary. The length of time over which data is retained will depend upon the circumstances, including the reasons why the personal information was obtained.

Staff shall follow QAHE's Records Management Policy and the relevant Data Retention Policy, or the criteria that is used to determine the retention period.

9. Incident Reporting and Management

All actual or suspected incidents of unauthorised disclosure, misuse, loss, alteration or destruction of personal data must be reported immediately in accordance with QAHE's established Security Incident Reporting procedure.

Suppliers must, where possible, initially report via the contractual reporting route to their QAHE contact. If that contact point is not available an incident should be reported to the QAHE IT Service Desk (0113 382 6200 Mon-Fri 08:00-18:00 UK time zone, or itservicedesk@qa.com).

Reported incidents are investigated and reported internally as appropriate and, where required, externally.

As appropriate, QAHE will:

- Make the required report of a data breach to the ICO (or the Data Controller) without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- When acting as a Data Controller, notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification required by law.

© 2026 QAHE Limited. All rights reserved.

10. Compliance

Any breach or attempted breach of this Policy may result in disciplinary action. This may extend to summary dismissal for employees or the termination of a contract for provision of services by a supplier.

Depending on the nature of the violation or attempted violation, individuals may also be held personally liable for civil or criminal penalties arising from their actions in line with UK or the appliable data protection legislation.

11. Policy Review and Maintenance

This Policy shall be reviewed annually or whenever there is a significant change that may affect its content, for example, legislation, strategy or organisation. The Policy Owner is responsible for initiating and coordinating the review of this policy in line with the Policy Framework.

© 2026 QAHE Limited. All rights reserved.


POWERING
POTENTIAL