

Author:	Samantha Hill	Version:	10
Edit Date:	06/10/2025	Review Date:	05/10/2026
Director Approval:	Leonie Walker		

NQual is committed to being transparent about how personal data is collected and used, ensuring they are meeting its data protection obligations. This policy sets out the company’s commitment to data protection and the individual’s rights and obligations in relation to how personal data is used throughout the organisation and assessment process.

This policy applies to all individuals whose personal data NQual processes, including current and former employees, workers, contractors, volunteers, apprentices, learners, assessors, IQAs, EQAs, centre staff and applicants. This includes individuals engaged on a permanent, fixed-term, temporary, casual or zero-hours basis.

Definitions

Data Protection Legislation

The General Data Protection Regulation (“GDPR”) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and (iii) any successor legislation to the GDPR or the Data Protection Act 2018.

Data Subject

A living identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data. This could be you, your colleagues, customers, suppliers or indeed any other person.

Personal Data

Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access, including but not limited to, data held in a filing system. Personal Data includes Special Categories of Data and Pseudonymised Personal Data, but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person’s actions or behaviour. This could include information in electronic, paper, or other formats (e.g., images, multimedia).

Personal Data Breach

Any breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of Personal Data.

How Will NQual Process Personal Data?

NQual will process personal data in accordance with the following data protection principles:

- NQual will process personal data lawfully, fairly and in a transparent manner.
- NQual will collect personal data only for specified, explicit and legitimate purposes.

- NQual will process personal data only where it is adequate, relevant and limited to what is necessary for processing.
- NQual will keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- NQual will keep personal data only for the period necessary for processing.
- NQual will adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

NQual will inform individuals of the reasons for processing their personal data, how it uses such data and the legal basis for processing in its Privacy Notices. It will not process the personal data of individuals for other reasons.

NQual will update personal data promptly when informed that information has changed or is inaccurate.

Personal data gathered during employment or engagement as a worker, contractor, volunteer, learner or whilst on an internship, is held in the individual's personnel file (hard copy, electronic format or both) and on HR systems. The periods for which the company holds personal data are contained in its Privacy Notices as issued to individuals at the point data is collected, or at other points as the company deems its obligations require.

Process For Requesting a Data Subject Access Request

All individuals have the right to make a subject access request. If an individual makes a subject access request, NQual will inform them about:

- Whether or not their data is processed and if so, why, the categories of personal data concerned and the source of the data if it is not collected from the individual.
- To whom their data is or may be disclosed, including recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers.
- For how long personal data is stored (or how that period is decided).
- Rights to rectification or erasure of data, or to restrict or object to processing.
- The right to complain to the Information Commissioner if the individual thinks the company has failed to comply with their data protection rights.
- Whether or not the company carries out automated decision-making and the logic involved in any such decision-making

NQual will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

To make a subject access request, the individual should send the request to quality@nqual.co.uk

In some cases, NQual may need to ask for proof of identification before the request can be processed. NQual will inform the individual if it needs to verify their identity and the documents it requires.

NQual will normally respond to a request within 30 days from the date it is received.

If an employee of NQual receives a Data Subject Access request, they must immediately inform the Chief Executive Officer (CEO) and take steps to comply with the above response procedure.

NQual recognises that, under UK employment law and data protection legislation, employees, workers and individuals engaged by NQual have specific rights in relation to their personal data.

Personal data processed during employment or engagement may include, but is not limited to:

- Recruitment and selection records
- Contracts and engagement records
- Payroll, tax and statutory payments
- Sickness absence and health-related records
- Family leave and statutory leave records
- Disciplinary, grievance and whistleblowing records
- Training, performance and quality assurance records

Such data is processed only where there is a lawful basis to do so, including **legal obligation**, **contractual necessity**, **public task**, **legitimate interests**, or **special category processing** where applicable.

NQual ensures that employment-related personal data is:

- Processed fairly and transparently
- Limited to what is necessary for employment and regulatory purposes
- Retained in accordance with statutory requirements and NQual's Record Retention Policy
- Accessed only by authorised personnel

Right to Complain About Data Processing

In accordance with the Data (Use and Access) Act 2025, individuals have the right to raise a complaint directly with NQual if they have concerns about how their personal data has been processed.

This right applies to employees, workers, learners, contractors, centres and any other data subjects whose personal data NQual processes.

Data protection complaints should be submitted to quality@nqual.co.uk and will:

- Be acknowledged promptly
- Be investigated fairly and objectively
- Receive a written response within a reasonable timeframe

Where an individual remains dissatisfied following NQual's response, they retain the right to escalate their complaint to the **Information Commissioner's Office (ICO)**.

Raising a data protection complaint will not result in any detriment, disciplinary action or unfavourable treatment against an employee, worker or learner.

How Will NQual Process Personal Data?

Everyone who works for, or on behalf of, the company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the company's Data Security and Data Retention policies.

The Managing Director is responsible for the implementation of any actions relating to this policy and updating all staff about their data protection responsibilities and any risks in relation to the processing of data. NQual employees should direct any questions in relation to this policy or data protection to this person. All NQual staff should always ensure the following in line with this policy:

- NQual employees should only access personal data if they need it for the work they do for, or on behalf of the NQual and only if they are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- NQual employees should not share personal data informally.
- NQual employees should keep personal data secure and not share it with unauthorised people.
- NQual employees should regularly review and, where required or requested, update personal data they deal with. This includes telling us if your own contact details change.
- NQual employees should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- NQual employees should use strong passwords and not share their passwords with any other person.
- NQual employees should lock their computer screens when not at their desks.
- NQual employees should consider anonymising data or using separate keys/codes so that the Data Subject cannot be identified.
- Do not save personal data to your personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of Ashley Robertson.
- NQual employees should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- NQual employees should not take personal data away from the company's premises without authorisation from the Managing Director.
- Personal data should be shredded and disposed of securely when you have finished with it.

If any NQual employees have concerns or are unsure about any aspect of data protection or security, they should ask for help from the Data Protection Officer/Data Protection Manager.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken against the staff member in accordance with the disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in dismissal.

For What Reasons Can Personal Data Be Collected or Processed?

- Personal data must be collected only for specified, legitimate purposes.
- Personal data cannot be used for new, different or incompatible purposes from that discloses when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

In an employment and engagement context, NQal processes personal data where necessary to:

- Comply with legal and statutory obligations, including employment law, payroll, statutory sick pay, family leave, holiday pay and safeguarding.
- Fulfil contractual obligations to employees, workers and contractors.
- Meet regulatory obligations as an Ofqual-recognised awarding organisation.
- Operate fair recruitment, disciplinary, grievance and whistleblowing processes.

Special category personal data, including health information, will be processed only where a lawful condition applies and appropriate safeguards are in place.

Is there a Limit to the Amount of Personal Data that can be collected and processed?

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed (Qualifications and Assessment).

- Personal data must only be processed when performing job duties require it. Processing personal data for any reason unrelated to your job duties is not permitted.
- Excessive data must not be collected. Ensure any personal data collected is adequate and relevant for the intended purposes.
- When personal data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the company's data retention guidelines.

Data Sharing

NQal will share data based on the following conditions:

- For the delivery of End-Point Assessment, we will share the following information with the Education and Skills Funding Agency and the Institute for Apprenticeships and Technical Education.
 - Learner name
 - Unique learner number
 - Date of birth
 - Employer name
 - Any other information required, including details of name changes, proof of changes and address where applicable
- Before an assessment, if reasonable adjustments are required, we will request details of the difficulty and/or disability in the context of the reasonable adjustment required. This data will be shared with your employer/centre and NQal to ensure that the reasonable adjustments can be agreed upon and put in place. No information on difficulties/disabilities can be submitted to NQal without the learner's consent.

- NQual will share your name and employer with the assessors so that we can check for any potential conflicts of interest in assessments.
- NQual will share anonymised data on assessment results with Ofqual and for our own monitoring and quality assurance purposes.
- For the award of Qualifications, we will share information with the Education and Skills Funding Agency and Ofqual.

Personal data received through whistleblowing or protected disclosure processes is handled with enhanced confidentiality and security.

In line with employment legislation, disclosures relating to matters such as sexual harassment, safeguarding, misconduct or regulatory breaches are processed under lawful bases, including **legal obligation** and **public interest**.

Whistleblowing records are:

- Access-restricted
- Retained in line with statutory and regulatory requirements
- Processed separately from routine HR records where appropriate

How Long Can Personal Data Be Stored?

Under guidance, personal data must not be kept longer than necessary for the purposes for which the data is processed. Certain employment-related records, including holiday pay and statutory leave records, are retained for a minimum of **six years** to meet legal and regulatory requirements.

What Should Happen in the Event of a Data Breach Occurring?

If NQual suspects or discovers that there has been a breach of personal data and that this could pose a risk to the rights and freedoms of individuals, we will report the breach to the Information Commissioner within 72 hours of discovery. NQual will record all data breaches regardless of their effect, and employees must therefore report any breach, regardless of any perceived level of severity.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, NQual will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

Centres and employees of NQual who become aware of or suspect that a personal data breach has occurred should not attempt to investigate the matter themselves. They should immediately contact the designated investigating officer at NQual for personal data breaches. All evidence relating to the potential personal data breach should be preserved. Failure to notify the designated person may result in sanctions against a centre or disciplinary action as applicable.

Third-Party Monitoring of Data Security

NQual's Centres use a variety of systems to store personal data, and these systems are subject to this GDPR policy. All Centres are required to have a GDPR policy in place that is in line with this policy and are responsible for complying with GDPR. NQual may perform spot checks to ensure that this policy is complied with by Centres.

NQual uses ACE360 for the storage of End-Point Assessment information. This contains personal details of learners and is also subject to monitoring under this policy. Ace360 has its own privacy policy, and a link to this can be found below:

<https://ace360.org/privacy-policy/>

Will NQual Take Disciplinary Action if there is a Data Breach?

No disciplinary action would automatically be taken simply because a breach has occurred. An investigation would first need to be carried out to establish the causes of the breach.

Where an investigation reveals that a data breach has been caused (wilfully or negligently or without due care and attention) through an employee's actions or inactions, this may lead to disciplinary action being taken. In the event of a serious breach and/or a failure to follow the appropriate procedures NQual has put in place for data processing, this could amount to an offence of gross misconduct.

Failure to report a breach or suspected breach could result in disciplinary action. In serious cases, this could amount to an offence of gross misconduct.

NQual uses secure portals for the collection and storage of data. For further information on data storage, contact www.ACE360.co.uk

All policies relate to qualifications and assessments conducted by NQual Ltd.

This policy will be reviewed annually as a minimum.