Data Protection Policy

Policy statement

QAA needs to collect personal information to effectively carry out our everyday functions and activities, and to provide our products and services. Such data is collected from employees, members, customers, suppliers and clients, and includes *(but is not limited to)* name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations. However, we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR), UK data protection laws and any other relevant data protection laws and codes of conduct (collectively referred to as **'the data protection laws'**).

QAA is committed to ensuring and maintaining the security and confidentiality of personal and/or special category data and all colleagues are responsible for handling data in accordance with this policy.

Scope

The purpose of this policy is to ensure compliance with the *Data Protection Act (DPA) 2018* and General Data Protection Regulation (GDPR) (EU) 2016/679, which govern any processing of information about living individuals and the rights those individuals have relating to this information. This legislation covers all personal information held in both electronic and manual form.

QAA is both a controller and processor of personal data and is registered with the Information Commissioner's Office (ICO) as a Data Controller. The policy incorporates guidance from the ICO and outlines how QAA will discharge its duties and obligations to comply with data protection legislation.

This policy applies to all parts of QAA and to all personal data held and processed by the organisation. This includes data held in any system or format, whether electronic or manual.

Adherence to this policy is mandatory for all employees of QAA including all permanent, fixed-term and temporary staff, reviewers, third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with QAA in the UK or overseas. Non-compliance could lead to disciplinary action.

Categories of data

For the purposes of information categorisation, QAA applies the GDPR definitions of 'personal data' and 'special category data', as follows:

Personal data	Special category data
Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as: • a name • an identification number • location data • an online identifier, or • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Personal data revealing or relating to an identifiable natural person's: • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • health • sex life or sexual orientation, or • the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person.

QAA ensures that personal data falling within the GDPR's **'special categories'** is handled with a particularly high level of care, due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to. The processing of special category data by QAA is kept to the minimum necessary to enable us to perform our functions.

Data protection principles

Article 5 (2) of the GDPR requires that QAA, its employees and others who process or use any personal information shall be responsible for, and be able to demonstrate, compliance with the data protection principles.

The data protection principles state that personal data should be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data is processed
- processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

QAA's policy is that the processing of all personal data should be safe, secure, ethical and transparent and we have procedures in place to enable data subjects to exercise their rights.

- We protect the rights of individuals with regards to the processing of personal information.
- We develop, implement and maintain a Data Protection Policy, procedure and training for compliance with the data protection laws.
- We record consent at the time it is obtained and evidence such consent where requested.
- We have robust and documented Complaint and Data Incident Reporting policies for identifying, investigating, reviewing and reporting any breaches or complaints about data protection.
- We store and destroy all personal information in accordance with our Retention Policy.
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- We maintain records of processing activities.

Records of processing where QAA is a Data Controller or Data Processor

Where we act in the capacity as a Data Controller or Data Processor (*or a representative*), our internal records of the categories of processing activities carried out will contain the following information:

- The full name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer.
- The categories of processing carried out on behalf of each controller.
- Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards).
- A general description of the processing security measures applied (pursuant to Article 32(1) of the data protection laws).

External certification

QAA is certified by the British Assessment Bureau to ISO 27001:2013 demonstrating that we are committed to, and actively managing, our data security provisions in line with international best practice.

Third-party processors

QAA uses external processors for certain processing activities. We use information audits to identify, categorise and record all personal data that is processed outside of QAA, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing may include (but is not limited to):

- IT Systems and Services
- Legal Services
- Payroll
- Financial Sustainability, Management and Governance Checks
- Direct Marketing/Mailing Services.

We have due diligence procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. In the course of these checks, we may obtain company documents, certifications and references to ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We ensure that Service Level Agreements (SLAs) and contracts containing appropriate compliance obligations are in place with all data processors via the contract approval process. Processors are notified that they must not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

It is the responsibility of the contract manager to ensure that each of the processing activities specified in the contract are monitored, audited and reported on.

Data subject rights

The rights given to data subjects under data protection legislation are:

- the right to be informed
- the right of access to the information held about them (through a Subject Access Request)
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision-making and profiling.

Under data protection legislation, data subjects have the right of access to their personal data held by QAA.

Any individual who wishes to exercise this right should make the request through submitting a Subject Access Request Form available on QAA's website, or by contacting Governance@qaa.ac.uk.

Data governance

Employee personal data

We do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information about how we process their data and why.

Privacy Notice

QAA's Privacy Notice includes what to expect when QAA collects personal information to meet our legal, regulatory, statutory and contractual obligations and to provide you with information, either about our products and services or about matters of public. The Privacy Notice also informs employees of their rights under the data protection laws and how to exercise these rights and details the personal information we collect and process about them. We also have a Privacy Notice for Payroll Processing that is published in the Policies section of our Intranet.

Data storage

Information and records relating to data subjects will be stored securely and will only be accessible to authorised employees. Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

Data accuracy

QAA takes reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

Audits and monitoring

We carry out regular audits and compliance monitoring processes with a view to ensuring that the measures and controls in place to protect data subjects and their information are adequate, effective and compliant at all times. QAA is accountable to the Audit and Risk Committee, and ultimately to the Board, in respect of compliance with this policy.

Training

QAA is committed to ensuring that all employees understand and have access to their obligations under data protection laws and principles, and that they have ongoing training and support to ensure and demonstrate their knowledge and competence.

New and existing employees are trained, assessed and supported to discharge their data protection responsibilities in a variety of ways, including:

- During induction.
- Every individual completes annual online training for GDPR and Cyber Security Awareness including a test at the end of each module.
- Annual refresher training covering data protection, records management and information security that is delivered in group sessions either-face to-face or virtually
- 1 to 1 support sessions.
- Access to data protection and information security policies, procedures, checklists and supporting documents.

Penalties for non-compliance

QAA understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any of these. We respect the Information Commissioner's authority to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees should note the severity of such penalties and their proportionate nature in accordance with the breach, including the following:

Type of breach	Maximum fine
Breaches of the obligations of the controller, the processor, the certification body and the monitoring body.	Administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, specific processing situations or non-compliance with an order by the Information Commissioner.	Administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Roles and responsibilities

As a Data Controller (or when acting as a joint Data Controller or a Data Processor), QAA has a corporate responsibility for:

- complying with data protection legislation and holding records to demonstrate this
- cooperating with the ICO, the UK regulator of data protection legislation
- responding to regulatory/court action and paying administrative levies and fines issued by the ICO.

Roles and responsibilities are defined as follows:

Chief Executive

QAA is a Data Controller and the Chief Executive is ultimately responsible for ensuring that the requirements of data protection laws are met and the organisation provides sufficient resources to enable the company and all employees to comply with their data protection duties.

Data & Information Governance Group (DIGG)

DIGG monitors compliance with data protection laws and with internal policies relating to data protection auditing. DIGG also reviews data protection, retention and records management policies and makes recommendations for Chief Executive approval.

Data Protection Officer (DPO)

QAA's Finance Director is the DPO and is responsible for:

- cooperating with the supervisory authority
- regular reporting to Executive/Board in context of operational and strategic risk identification and management.
- submission of annual reporting of performance to QAA's Audit & Risk Committee.

Facilities & Compliance Manager

- Refers to external legal advisers and Jisc subject matter experts as appropriate.
- Investigates data incidents and reports findings and recommendations to the DPO.
- Advises on data protection impact assessments and monitors the performance of the assessments.
- Oversees data records management and employee training.

Employees

It is the responsibility of all employees to:

- ensure that they collect, store and process personal data in accordance with data protection laws and comply with QAA's Data Protection Policy
- only use personal data for the purpose of their contracted duties
- keep personal data secure, including following applicable company policies and processes
- store contacts in approved and managed systems and not held in duplicate copies elsewhere
- not attempt to gain access to information that it is not necessary for them to hold, know or process
- ensure that any personal data obtained is accurate and relevant to the purpose for which it is required
- successfully complete mandatory training.

Policy review

This policy will be updated as a minimum on a two-yearly basis or as necessary to reflect best practice, relevant case law, and to ensure compliance with any changes or amendments to data protection legislation.

Published - 10 June 2021