Title of policy: **Data Protection Policy**
Policy statement (summary of main points) Sets out QAA's overarching approach to the protection of data about individuals. Covers: • Definition and categories of data • Data processing principles • Data protection processes and procedures • Access to individual rights in respect of personal data • Data Transfers • Cross-agency responsibilities for data protection
Strategic aim of the policy (link to corporate aim or group/team strategic aim) The purpose of this policy is to ensure that QAA meets its legal, statutory and regulatory requirements under the data protection laws in the conduct of its operations, and to ensure that all personal and special category information is processed compliantly.
Link to other policies / procedures and guidelines: • Information Security Policy • Information Retention Policy and Schedule • Data Rectification and Erasure Policy • Information Incident Reporting Policy • Data Audit Register • Privacy Notices • Information Request Policy

Created/owned by: Governance Team	
Approved by: QAA Executive	
Date last reviewed / updated	April 2018
Date next review due	2 years from approval
Location: Risk site	Version: 8.0
For further information contact	Lavinia Blackett, Head of Governance Graham Hardy, Head of IT

CONTENTS

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, 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 members of staff are responsible for handling data in accordance with this policy.

Scope

This policy applies to all staff within QAA which, for the purpose of this policy means all permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with QAA in the UK or overseas. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

General Data Protection Regulation (GDPR)

As QAA processes personal information regarding individuals (*data subjects*), we are obliged under GDPR to protect such information, and to obtain, use, process, store and destroy it, only in compliance with GDPR's rules and principles.

Categories of data

For the purposes 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 • to 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, • the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, • data concerning health, or • data concerning a natural person's sex life or sexual orientation

QAA ensures that personal data falling within the GDPR's "***special categories"*** *(previously known as sensitive personal data*) 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

QAA processes, and ensures that any party undertaking processing on its behalf also processes, all personal data in accordance with the requirements of GDPR.

All personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (**'purpose limitation'**)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (**'data minimisation'**)
- accurate and, where necessary, kept up to date; (**'accuracy'**)
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (**'storage limitation'**)
- 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 (**'integrity and confidentiality'**).

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

Data Governance Procedures

Accountability & compliance

We carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of personal data processing. These are overseen by the Data and Information Governance Group (DIGG), which receives and comments on the findings and ensures that recommendations are implemented.

We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws, as specified in our information security policies.

Privacy by Design

We operate a *'Privacy by Design'* approach, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures *(detailed below*), that help us enforce this approach.

Data Minimisation

Our systems, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose.

Pseudonymisation

In some cases we use pseudonymisation to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (*personal identifiers*). Encryption and partitioning is also used to protect the personal identifiers, which are kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation can mean that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption

We use encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We use encryption for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Head of IT or Director of Resources is required to authorise the transfer and review the encryption method for compliance and accuracy.

Hard Copy Data

It is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (*i.e. copies of student records, attendance lists, or other evidence collected in the course of our review visits*). Where this is necessary, we will normally digitise the data as soon as reasonably practical, apply the

appropriate retention period to the digitised version, and securely destroy the hard copy.

Legal basis for processing (Lawfulness)

All personal information processing activities undertaken by QAA must be permitted under one or more of the legal bases for processing such information contained within GDPR.

The legal basis for processing must be identified in the course of the Data Privacy Impact Assessment for the activity (see below) and documented. It should also be included in Privacy Notices and, where applicable, provided to the data subject and Information Commissioner as part of our information disclosure obligations.

Data is only obtained, processed or stored lawfully when one or more of the following applies: **-**

- The data subject has given **consent** to the processing of their personal data for one or more specific purposes
- 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
- Processing is **necessary for compliance with a legal obligation** to which we are subject
- Processing is **necessary in order to protect the vital interests of the data subject** or of another natural person
- Processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in QAA
- Processing is **necessary for the purposes of the legitimate interests pursued by QAA** or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data*).*

Processing Special Category data

We will only ever process special category data where one or more of the following applies:

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is carried out in the course of our legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Where QAA processes personal information that falls into one of the above categories, we will do so in accordance with the provisions of the law.

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

Where we act either in the capacity as a data controller or in the capacity as a 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 utilises 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
- 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 and compliant 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 retention & disposal

QAA has defined procedures for adhering to the retention periods set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. Please refer to our Information Retention Policy for full details on our retention, storage, periods and destruction processes.

Data Protection Impact Assessments (DPIA)

Part of QAA's privacy by design approach requires that impact on data subjects is thoroughly considered in advance of undertaking new types of processing.

A Data Protection Impact Assessment (DPIA) must be undertaken in any of the following circumstances:

- Where QAA is considering carrying out a new activity involving data processing;
- Where QAA is considering processing that utilises new technologies; and/or
- Where there is a likelihood that processing could result in a high risk to the rights and freedoms of data subjects.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

Please refer to our **DPIA Procedures** for further details.

Data Subject Rights Procedures

Consent & The Right to be Informed

QAA has specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws. Consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Where QAA processes data on the basis of consent, the following principles apply:

- Consent requests are transparent, written in plain language and do not contain illegible terms, jargon or extensive legal terms
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data
- Pre-ticked, opt-in boxes are never used
- Where consent is given as part of other matters (i.e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters and is not a precondition of any service (unless necessary for that service)
- Along with our company name, we also provide details of any other third party who will use or rely on the consent
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our company name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: -
    - Opt-out links in mailings or electronic communications
    - Opt-out process explanation and steps on website and in all written communications
    - Ability to opt-out verbally, in writing or by email

Methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear.

Privacy Notices

QAA defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal data (or at the earliest possible opportunity where that data is obtained indirectly*)*.

QAA Privacy Notices must be based on the standard template to ensure that they contain the information required by law.

The Privacy Notice is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

We have links to our Privacy Notices on our website and can provide a copy of physical and digital formats upon request.

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.

An employee Privacy Notice which informs staff 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 is published on the policies section of the intranet.

The Right of Access

QAA facilitates the right of data subjects to access information that we hold about them through our information request procedure. Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity.

The Right to Data Portability

QAA does not envisage that the types of information that it processes about individuals will be subject to requests to exercise the individual's right to data portability, but where any such request is made, QAA is committed to providing the requested personal data pertaining to the data subject to them on request and in a format, that is easy to disclose and read.

Where requested by a data subject and if the request meets the necessary conditions as specified by GDPR, we will transmit the personal data directly from QAA to a designated controller, where technically feasible.

All transmission requests under the right to portability must be assessed to ensure that no other data subject is concerned.

The Right to Rectification

All data held and processed by QAA is reviewed and verified as being accurate wherever possible and is always kept up to date. All staff have responsibility for ensuring that QAA data is accurate.

Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

Please refer to the Rectification and Erasure of Data procedure for details.

The Right to Erasure

Also, known as *'The Right to be Forgotten'*, QAA complies fully with the right of individuals to request the erasure of their data from our systems, and ensures that personal data which identifies a data subject is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by QAA is categorised when assessed by the Data Protection Impact Assessment and is either given an erasure date in accordance with the Information Retention Policy or is monitored so that it can be destroyed when no longer necessary.

Please refer to the Rectification and Erasure of Data procedure for details.

The Right to Restrict Processing

There are certain circumstances where QAA restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.
Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.
QAA will apply restrictions to data processing in the following circumstances: -

- Where an individual has contested the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Head of IT or the Director of Resources must review and authorise all restriction requests and copies of notifications from and to data subjects and relevant third-parties must be retained.

Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Information Commissioner and to a judicial remedy.

The Right to Object to processing

Where applicable, data subjects are informed of their right to object to processing in our Privacy Notices. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online.

Individuals have the right to object to: -

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (*including profiling*)
- Processing for purposes of scientific/historical research and statistics

Where QAA processes personal data for the performance of a legal task, in relation to our legitimate interests (including the discharge of our public functions) or for research purposes, a data subjects' objection will only be considered where it is on *'grounds relating to their particular situation'*. We reserve the right to continue processing such personal data where: -

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- The processing is for the establishment, exercise or defence of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, QAA will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

Oversight Procedures

Security & breach management

Alongside our 'Privacy by Design' approach to protecting data, we ensure the maximum security of data that we process, including when it is shared, disclosed and transferred. Our information security policies provide the detailed measures and controls that we take to protect personal information and to ensure its security.

Whilst every effort and measure are taken to reduce the risk of data breaches, QAA has dedicated controls and procedures in place for implementation in such situations, along with the notifications to be made to the Information Commissioner and data subjects (where applicable). Please refer to our Data Incident Reporting Policy.

Transfers & data sharing

Where data is being transferred for a legal and necessary purpose, compliant with GDPR, it must be transferred via a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation requirements.

We use approved, secure methods of transfer and all data being transferred is noted on our information audit so that tracking is possible, and authorisation is accessible. The Head of IT or Director of Resources must authorise all EU transfers and verify the encryption and security methods and measures.

Audits & 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 staff understand, have access to and can easily interpret 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 the induction process
- GDPR Workshops & Training Sessions
- Annual online training and assessment
- 1:1 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

Responsibilities

Responsibilities for certain areas of data protection have been allocated across QAA as follows:

Responsibility	Details of responsibility	Undertaken by	Reporting channels

Expert Advice	Inform and advise the organisation and employees carrying out processing of their obligations under the GDPR and other EU or member state data protection provisions.	**External Legal Advisers** **Governance Officer** **Head of Governance**	Regular reports to Executive Committee/Board in context of termly legal.
Compliance Monitoring	Monitor compliance with the GDPR and other relevant laws, and with internal policies relating to data protection auditing.	**Data & Information Governance Group**	Regular reports to DIGG
Data Protection Impact Assessments	Advise on data protection impact assessments and monitoring the performance of the assessments	**Governance Officer** **Head of Governance** **Head of Information Security**	Work to be overseen by DIGG, and completed assessments stored on DIGG site. Escalation to Executive if required. Annual report to Executive/Board on performance of assessments
Risk	For all tasks, QAA must have due regard for the risks associated with the processing operations.	**External Legal Advisers** **Governance Officer** **Head of Governance**	Regular reporting to Executive/Board in context of operational and strategic risk identification and management.
Supervisory authority	Cooperating with supervisory authorities, acting as point of contact on issues relating to processing, including prior consultation.	**Head of Governance**	Directly to Board/Chairman as required.
Record Keeping	QAA must create inventories and hold registers of processing operations, based on the information provided to them by various departments within the organisation	**Governance Team** **Contract Managers**	Regular status reports to Head of Governance / Executive / Audit Committee.
Policy implementation	Application of the data protection principles enshrined in this policy	**All Staff**	To line managers or in accordance with the applicable policy.