Data Protection

Version number	v8.1
Policy author	Kirsty Hurt, Data Protection & Records Manager
Policy owner	Michael Baxter, Director of Finance & Corporate Services
Business Area	Strategic Planning & Governance
Policy effective from	December 2022
Policy review date	November 2024
Policy approved by	Information Governance Steering Group
Policy approval date	20 December 2022
Equality impact assessment (EqIA) approval date	1 December 2022

Why do we need the policy?

The purpose for the policy is to provide a framework to support SQA's compliance with data protection laws and to demonstrate how SQA will meet the data protection principle on accountability.

Who is it for?

This policy applies to all users of SQA's information and information systems (employees, agency workers, consultants, and others with authorised access to SQA's information or information systems)

What support is available?

Contact the information governance team at information.governance@sqa.org.uk

1. Introduction

This policy forms part of a suite of policies that support the effective and safe use of SQA's information and information systems.

UK data protection law puts the rights of individuals at the centre of processing decisions. The emphasis is on protecting citizens and their data and giving individuals more information about, and control over, how their personal data is used.

SQA must comply with data protection laws and be able to provide evidence of compliance to meet the requirement for accountability. SQA must ensure that all users of personal data are made aware of SQA's legal obligations for processing personal data and of their individual responsibilities.

SQA is committed to equality of opportunity and to a culture that respects difference. We believe that, as an employer and public body, we can play a leading part in promoting equality, diversity and inclusion by making them an integral part of our decision making. This policy has an Equality Impact Assessment completed on it at the development stage to assess how this policy may impact on equality groups and the findings from this are reflected in this policy.

2. Purpose

This policy provides a framework to support SQA's compliance with data protection law and to demonstrate how SQA will meet the data protection principle on accountability.

3. Scope

This policy applies to all personal data held by SQA and includes (but is not limited to) information about:

- Candidates and their parents or guardians
- Employees and ex-employees of SQA and predecessor bodies
- Agency workers and consultants (current and former)
- Applicants for SQA positions, appointee roles or other positions (successful and unsuccessful)
- Other workers – temporary, short-term and voluntary work placements
- Individuals working for our suppliers, partners or in centres

Data protection laws apply to recorded information or to images (for example, photographs or CCTV footage) that allow individuals to be identified.

4. Definition of Personal Data

Personal data means any information relating to an identifiable individual (known as a data subject) who can be identified, directly or indirectly, by reference to an identifier. An identifier could be a name, ID number, location data or online username.

This means personal data is information that relates to an identified or identifiable individual.

Some personal data is considered more sensitive in nature and requires a higher level of protection. These are called ‘special categories of personal data’ or ‘special category personal data’. This means personal data about an individual’s:

- race
- ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- genetic data
- biometric data (where it is used for ID purposes)
- health data
- sex life or sexual orientation

SQA considers transgender information as special category personal data.

Although not defined as special category personal data, information about someone’s criminal convictions and offences also requires a higher level of protection.

Any processing of these categories of personal data must comply with this policy and the Processing of Special Category and Criminal Data Policy. Before collecting or using any of these categories of personal data for the first time or for a new purpose, users must seek advice from the data protection team.

5. Responsibilities

All SQA appointed users of personal data must comply with data protection laws and this policy.

5.1 *Employees, agency workers, secondees, consultants*

Individuals are responsible for

- ensuring that they understand and comply with the requirements of data protection laws and this policy in relation to their role or contract
- using personal data only in accordance with their role or contract
- adhering to internal guidance on information management and any other instructions provided to them in relation to their role or contract
- undertaking data protection training:
    - new employees are required to read and confirm understanding of the Data Protection Policy and to complete the data protection module on SQA Academy within 28 days of joining SQA
    - all employees are required to complete data protection training when directed by the Information Governance team

5.2 *Line Managers*

Line managers are responsible for

- ensuring that access to personal data is controlled and only given to individuals in accordance with their duties or contractual responsibilities

- ensuring that access to personal data is removed promptly where a change in post, duties or contractual responsibilities results in an individual no longer requiring access

- reporting any security incident, 'near miss or data breach on becoming aware of them and in accordance with the Security Incident Management procedures

- ensuring that individuals under their line management are aware of their responsibilities for personal data as set out in this policy and other related policies

5.3 *Data Protection Team*

SQA's data protection team is responsible for

- advising on data protection queries or issues

- receiving and managing data subject requests

- managing and updating SQA's record of processing activities and privacy information

- managing the process for data protection impact assessments (DPIA)

- managing the process for data sharing where this relates to personal data

- implementing the process for transfer risk assessments

- developing, managing and reviewing data protection policies, processes and practices required to demonstrate compliance with data protection law

- liaising with SQA's legal advisors where complex data protection issues require specialist advice

5.4 *Data Protection Officer*

SQA's Data Protection Officer is responsible for

- advising on and monitoring compliance with data protection law and with policies in relation to the protection of personal data

- awareness raising and training of staff involved in processing operations

- conducting audits to demonstrate compliance

- providing advice on data protection impact assessments (DPIA) and monitoring SQA's performance on DPIAs

- acting as the contact point for the Information Commissioner's Office on issues relating to the processing of personal data and data breach reporting

For advice, contact the data protection team or Data Protection Officer at data.protection@sqa.org.uk.

5.5 *Heads of Service*

Heads of Service are responsible for

- ensuring that staff in their business area do not process personal data for any new or different purposes without first contacting a member of the Data Protection team
- ensuring that any reports of an actual or suspected data breach are reported immediately in accordance with the Information Security Incident procedures
- ensuring that individuals appointed for specific contracts (for example, appointees, agency workers) are provided with appropriate information about data protection and confidentiality on appointment, induction and during their contracted period of appointment
- ensuring that personal data processed by staff in their business area is included in the SQA Retention Schedule and that this is consistently applied to ensure that personal data is not kept longer than needed
- co-operating with the Data Protection Officer to review SQA's Privacy Statement and Record of Processing and in carrying out audits on the requirements of all data protection law

5.6 *Senior Information Risk Owner*

SQA's Senior Information Risk Owner (SIRO) is the Director of Finance and Corporate Services. The SIRO is responsible for

- leading a culture of good information management
- owning policies and processes related to information risk
- advising the Chief Executive on information risks

6. Processing Purposes and Lawful Basis

Data protection law requires SQA to specify the reasons and have a lawful basis for processing (using) personal data. To be lawful SQA's processing of personal data must meet at least one of the following conditions:

- It is necessary in order to carry out a specific task in the public interest or to exercise official authority (public task or statutory function).
- It is necessary to meet a legal obligation.
- It is necessary for a contract.
- The data subject (individual) has given their consent.

- It is necessary to protect someone's vital interests, that is, protecting someone's life.
- It is necessary for the legitimate interests of the controller or a third party.

Where special category personal data is being processed, SQA must also meet one of the following conditions:

- The data subject (individual) has given their explicit consent.
- It is necessary for employment, social security or social protection purposes.
- It is necessary to protect someone's vital interests, that is, protecting someone's life.
- The processing is being carried out by a not-for-profit body (charity)
- The personal data has been made public by the data subject (individual)
- It is necessary for legal claims
- It is necessary for reasons of substantial public interest (these reasons are detailed in the Data Protection Act 2018)
- It is necessary for health or social care
- It is necessary for public health
- It is necessary for archiving, research or statistics purposes.

SQA's Privacy Statements and Record of Processing explain the reasons and lawful basis for all our processing of personal data. Both are available on our website and a separate Privacy Statement for employees is available in the HR pages on the Intranet.

When SQA collects personal data from individuals, we must provide them with a privacy statement to let them know how and for what purpose we are using their personal information. That privacy statement must include the following:

- Identity and contact details of the controller
- Purpose of the processing and the lawful basis for the processing
- Categories of personal data
- Sources of personal data
- Recipients of the personal data
- Details of international transfers and associated safeguards
- Retention periods
- Individuals' rights including the right to complain to the ICO

SQA's Privacy Statements fully reflect our processing of personal data. Any proposal to use personal data for a different purpose to that stated in the Privacy Statement or Record of Processing, or a new requirement to collect additional personal data, must be discussed with SQA's Data Protection Team.

7. Compliance with data protection principles

The data protection principles are central to data protection law and key to meeting its requirements. They are a fundamental building block of good data protection practice and must be followed by all SQA users of personal data. Any departure from these principles could put the personal data SQA processes at risk and lead to non-compliance with or breach of data protection law.

If any user of personal data believes that any current or planned processing is not in accordance with any of the principles below, they must seek advice from the data protection team.

7.1 *Personal data should be processed lawfully, fairly and in a transparent manner*

SQA must not process personal data

- without having a lawful basis, for example, public task, legal requirement, contract, consent*
- in a way that the individual wouldn't reasonably expect
- without telling the individual what personal data we hold about them, our reasons for processing their personal data, and anyone we will share their personal data with, unless an exemption applies

*Consent is unlikely to be the most appropriate lawful basis for processing personal data so must not be used without first contacting the data protection team.

7.2 *Personal data should be collected for specified, explicit and legitimate purposes*

SQA must be clear about, and record, the purpose(s) for processing. Personal data must not be processed for a reason that is incompatible with the purpose for which it was originally collected. If there is any need or plan to use personal data in a way that it is not currently used, contact a member of the data protection team for advice.

7.3 *Personal data should be adequate, relevant and limited to what is necessary*

SQA must not obtain personal data that isn't needed to achieve the identified purpose(s). Where information is needed only for a subset of individuals, it should only be requested for that particular subset.

7.4 *Personal data should be accurate and where necessary kept up-to-date*

SQA must take all reasonable steps to ensure that personal data is accurate and kept up-to-date; inaccuracies should be corrected promptly.

7.5 *Personal data should be kept for no longer than is necessary*

Personal data processed by SQA must be included in the SQA Retention Schedule. This must be consistently applied to ensure that personal data is destroyed when it is no longer needed.

The disposal of personal data must be undertaken in accordance with the Retention and Disposal Policy and procedures to ensure it is carried out securely.

7.6 *Personal data should be processed in a manner that ensures appropriate security*

SQA is responsible for the confidentiality, integrity and availability of the personal data it holds. SQA must ensure that appropriate technical and organisational

measures are in place in all aspects of its processing activities to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage. This includes (but is not limited to) the following measures:

- exercising due diligence in the recruitment or engagement of employees, appointees, contractors, suppliers and others to ensure their reliability
- ensuring access to personal data is controlled based on job role or contract
- ensuring that internal processes for the management of data are adequately communicated and followed by business teams; this includes data sharing and data protection impact assessment
- ensuring that employees and other relevant groups receive appropriate information at induction and at regular intervals to remind them of their responsibilities
- enforcing SQA's decision not to allow employees to use personal devices or personal email for SQA business purposes. Further information about this is included in SQA's Information Security Policy.

7.7 *Accountability Principle*

SQA, is required to take responsibility for and must be able to demonstrate compliance with the data protection principles set out in 7.1 to 7.6 above. All SQA users of personal data must therefore comply with this policy and any request from the data protection team for information or evidence of that compliance.

8. General Obligations

Data protection law includes further specific obligations, and these are set out below.

8.1 *Data Protection by Design and Default*

To implement the data protection principles and safeguard individuals' rights, SQA must build appropriate technical and organisational measures into all our processing activities. This means that employees must

- consider the privacy needs of individuals and other data protection issues when developing or reviewing systems and processes; and
- comply with requirements set out in SQA's project management and procurement procedures

8.2 *Record of Processing*

SQA's Record of Processing sets out all SQA's processing activities. This is a mandatory requirement and must include the following information:

- Details about the controller and the data protection officer
- Purposes of the processing of personal data
- Categories and descriptions of the personal data
- Categories of recipients of personal data in the UK and internationally
- Transfers of personal data and suitable safeguards
- General description of technical and organisational measures

The Record of Processing must be kept up-to-date. To ensure this happens

- the Data Protection Team will carry out regular reviews, and
- employees must assist with these reviews and contact the Data Protection team to advise of any changes out with them

8.3 *Security of Processing*

SQA must put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing. This means:

- pseudonymising and encrypting personal data, where appropriate
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- having the ability to restore the availability and access to personal data in a timely manner in the event of an incident
- having a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing
- ensuring that anyone who has access to personal data does not process that information unless they have authorisation
- complying with SQA's requirements around physical security measures

8.4 *Processors (for example, suppliers)*

Where processing of personal data is to be carried out by an external organisation SQA must only use suppliers that implement appropriate technical and organisational measures to ensure the protection of individuals' rights and a level of security appropriate to any risk associated with the processing.

Employees must comply with procurement procedures to ensure this obligation is met by SQA.

8.5 *Personal Data Breach*

Actual and suspected personal data breaches must be reported immediately. the Security Incident Reporting Procedure provides further information.

Employees, agency workers, consultants, and other authorised users

- Must report an incident immediately to their line manager
- Complete and submit a Security Incident Report Form

Incidents involving Appointees

- Appointees must be advised to report an incident immediately to the Appointee Services Manager at am@sqa.org.uk.

- Appointee Services Manager or Head of Service to complete and submit a Security Incident Report Form.

SQA's Data Protection Officer must notify the Information Commissioner's Office of a "reportable" data breach within 72 hours. A range of factors will determine if a breach needs to be reported to the ICO and if the individuals affected by a breach need to be advised. The data protection team is responsible for personal data breaches. They will review them to determine if and what actions need to be taken.

If an incident is suspected as being very serious the individual should inform their Head of Service Immediately. Significant incidents are likely to be reportable to the ICO and may result in an Incident Management Team being invoked.

8.6 *Data Protection Impact Assessment (DPIA)*

A Data Protection Impact Assessment (DPIA) is a mechanism for identifying the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stage and throughout the lifecycle of an initiative. A DPIA must be carried out where new technologies are being used and where there is a potential risk to the privacy and rights of individuals.

SQA has decided that a DPIA should be carried out for all new and changed projects, processes and contracts that involve the processing of personal data as well as in relation to some data sharing requests. Information about DPIAs and the Privacy Impact Review Group (PIRG) that review them is available on the Intranet.

The Data Protection Officer oversees and advises on DPIAs. Queries relating to DPIAs should be directed to the Data Protection Officer.

9. Individuals' Rights

Individuals have a number of rights under data protection law and SQA must ensure that its systems, policies, processes and practices are designed to enable individuals to exercise them.

Internal processes are in place to respond to individuals' rights requests. Some of these rights are conditional. SQA's Privacy Statement and the privacy statement for employees and secondees provide more information about the circumstances in which these rights apply. Therefore, it is important that the data protection team are involved where directed. Guidance is available.

9.1 *Right to transparency*

An individual has the right to be told about SQA's collection and use of their personal data. Information must be concise, understandable, written in clear and plain language and easily accessible.

- Employees need to ensure that, all guidance documents, forms (paper and electronic), letters and instructions, that are used to collect personal data, or contain references to the processing of personal data, comply with this requirement.

- The Data Protection Officer will be responsible for ensuring that SQA's Privacy Statements are compliant.

9.2 *Right to access personal data held about them (Subject Access Request)*

An individual has the right to request access to the personal data SQA holds about them; this includes information held by suppliers on behalf of SQA. This is known as a subject access request.

A subject access request may be submitted using our online form or received by email, phone call or letter.

- Employees must pass any requests from individuals for their personal data that are not normal business practice, to the data protection team who will ensure that each request is handled in accordance with our legal obligations.

- The data protection team will liaise with the requester or third-party who may have submitted a request on their behalf; and with the business team(s) responsible for providing the information.

- SQA must respond to subject access requests within one month of receiving valid requests.

9.3 *Right to rectification*

An individual has the right to request that any inaccurate personal data we hold about them is corrected.

- Employees should correct personal data where this is normal business practice or pass the request to the data protection team where it is not.

- The data protection team will review the request and liaise with the requestor and business team(s) responsible for correcting the information.

9.4 *Right to erasure*

An individual has the right to request erasure of their personal data. This is a conditional right that only applies in specific circumstances

- Employees must pass any request for erasure of personal data to the data protection team who will review the request and liaise directly with the requester and business team(s), where required.

9.5 *Right to restriction of processing*

An individual has the right to restrict processing of their personal data. This is a conditional right that only applies in specific circumstances.

- Employees must pass any request to restrict the processing of personal data to the data protection team who will review the request and liaise directly with the requester and business team(s), where required.

9.6 *Right to data portability*

An individual has the right to receive their personal data in a structured, commonly used and machine-readable format and have the right to transmit that data to another organisation. This is a conditional right that only applies in specific circumstances.

- Employees must pass any request for data to be provided in a portable format to the data protection team who will review the request and liaise directly with the requester and business team(s), where required.

9.7 *Right to object*

An individual has the right to object to the processing of their personal data and have it stopped in specific circumstances.

- Objections to the processing of personal data for direct marketing will normally be dealt with by the Marketing team. Where an individual objects to direct marketing processing of their personal data for this purpose must stop immediately.

- Employees must pass other objections to the processing of an individual's personal data to the data protection team who will review the request and liaise directly with the requester and business teams, where required.

9.8 *Right not to be subject to automated decision-making or profiling*

An individual has the right not to be subject to automated decision making and/or profiling. These are decisions or evaluations of certain things about an individual made solely by automated means and that do not have human involvement (for example, online credit applications or e-recruiting practices without human intervention).

Any plans to introduce automated processing must be subject to a Data Protection Impact Assessment.

10. Transfers of Personal Data out with the UK

There are potential risks to individuals' privacy when personal data is processed out with the UK.

Employees must contact the Data Protection Officer if they identify any **new** requirement or proposal to transfer/process personal data out with the UK as a transfer impact assessment will be required. This also applies to contracts with new and existing suppliers.

Before transferring personal data out with the UK, SQA must comply with the conditions of transfer set out in the UK GDPR to ensure that appropriate safeguards are in place.

11. Data Sharing

SQA shares personal data with organisations such as local authorities, UCAS and the Strathclyde Pension Fund. This sharing relates to the purpose for which the personal data was originally collected. Personal data is also shared with suppliers where it is necessary for the performance of their contract with SQA. Information about this sharing is set out in the Record of Processing.

An organisation or individual can request that SQA share personal data with them if they have a legitimate reason for processing the information. All requests for data sharing are subject to review and approval by the data protection team to ensure that requests meet the minimum standards required to share personal data including having an appropriate legal basis, and to enable a data sharing arrangement to be put in place where required.

A Data Sharing Request form must be completed and submitted to data.protection@sqa.org.uk for review by the data protection team. They may determine that a DPIA is required before the data sharing can proceed and will inform you of this.

12. Direct Marketing

Marketing is the communication of material about the sale of products and services as well as the promotion of aims and ideals. It covers communication sent in all forms such as by post, fax, telephone, text or email.

SQA must comply with all relevant legislation every time we undertake marketing. Personal data collected and used by SQA for the purposes of sending marketing communication must comply with data protection laws. In addition, any marketing sent by email or text must also comply with the Privacy and Electronic Communications Regulations 2003.

In particular, SQA cannot send marketing by email or text to an individual, unless we have obtained their consent and we must stop all direct marketing activities if an individual requests us to stop. This includes individuals operating as sole traders or as part of a partnership.

It doesn't include individuals working for an organisation or body where the marketing is being sent on a business-to-business basis. In these instances, the consent of the individual is not needed.

13. Compliance

A breach of this policy is a disciplinary offence and may constitute gross misconduct.

Under the Data Protection Act 2018 it is a criminal offence for any employee, appointee, agency worker, consultant, or other authorised person to access, use or disclose personal data without being authorised to do so for the purpose of their role or their contract. This may result in criminal prosecution.

14. Related SQA Policies and Legislation

This policy should be read in conjunction with the following SQA policies which are reviewed and updated as necessary to meet SQA's business needs and legal obligations.

- Processing of Special Category and Criminal Offence Data Policy
- IT Acceptable Use Policy
- Information Security Policy
- Email Policy
- Clear Desk and Clear Screen Policy
- Access Control Policy
- Freedom of Information Policy
- Records Management Policy
- Retention and Disposal Policy
- Anti-bribery and Corruption Policy
- CCTV Policy
- Home Based Worker Policy
- Disciplinary Policy

The following documents are also relevant.

- Record of Processing Activities (ROPA)
- SQA Privacy Statement
- SQA Employee and Secondee Privacy Statement
- Security Incident Management Procedures
- SQA Retention Schedule

This policy respects and complies with the following applicable laws.

- United Kingdom General Data Protection Regulation
- Data Protection Act 2018
- EU General Data Protection Regulation (2016/679)
- Human Rights Act 1998
- Computer Misuse Act 1990

15. Definitions

The following key concepts are important in understanding this policy.

Personal data is information that relates to an identified or identifiable individual – someone you can distinguish from others. The information that identifies someone can be as simple as a name or a number, or it could be another less obvious identifier,

such as an IP address or social media handle, or even a combination of identifiers such as a name and date of birth. Examples include

- name
- date of birth
- home address
- email address
- SCN — Scottish Candidate number
- NI — National Insurance number

Special category personal data means personal data that relates to:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- physical or mental health or condition
- sex life or sexual orientation
- genetic data
- biometric data (where it is used for ID purposes)

Note: SQA considers transgender information to be special category personal data, it must therefore be treated as such.

Processing includes creating, obtaining, recording, storing or using the personal data – anything from getting it, moving it, analysing it, reading it, sharing it with anyone, storing it, deleting or destroying it.

Controller refers to an organisation or individual who decides the purpose and manner in which personal data should be processed.

Processor is an organisation or an individual who processes personal data on behalf of a controller, for example, printer, courier, IT contractor.

Data subjects are living people (individuals) about whom the personal data relates.

Data subject request is a request from an individual (data subject), or an authorised third party, to exercise one of their rights under data protection law. This includes a subject access request, known as a SAR, which is a request for access to personal data processed about them.

Incompatible purpose is a purpose that is either very different from the original purpose, would be unexpected, or would have an unjustified impact on individuals.

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

Technical security measures are measures to protect information held on systems, such as network security, malware prevention, encryption and back-ups.

Organisational security measures support technical measures, and include policies and procedures, training and awareness, and access controls.

Pseudonymisation is where information fields within a data record are replaced by one or more artificial identifiers or pseudonyms. This masks information without it being completely anonymised.