SQA Data Protection Policy

Policy	SQA is committed to adopting best practice in protecting the personal information of all candidates, employees, appointees, nominees, agency workers, secondees, consultants, and employees of customer, partner and supplier organisations. This policy sets out SQA's approach to comply with legal requirements and maintain the confidence of those individuals who trust SQA with their personal information.
Why do we need this policy?	The purpose of the Data Protection Act 1998 is to protect individuals from having their personal data or privacy exploited or abused. This places the onus on organisations and individuals processing such data to ensure that the processing is conducted in a fair, lawful and secure way. It is therefore of vital importance that all SQA employees, appointees, nominees, agency workers and secondees comply with the requirements of the Act.
What does the policy apply to?	This policy applies to all: ♦ employees ♦ appointees and nominees ♦ agency workers ♦ secondees ♦ suppliers ♦ consultants As a public body, the Act applies to all recorded information about living individuals held by SQA. This includes (but is not limited to) information about: ♦ employees and ex-employees (or agency workers or secondees) of SQA and predecessor bodies ♦ appointees and nominees ♦ candidates or their parents/guardians

	♦ individuals working in centres or other awarding bodies, or attending events ♦ individuals working for our suppliers or partners The Act applies equally to images (eg photos or CCTV footage) or recorded audio information that allows individuals to be identified, as to written information. One person's opinion about another individual is personal information about both of them. It applies whether the individual is located in the UK, European Economic Area or worldwide.
Which parts of SQA are affected?	The Act applies to any 'processing' of personal information. This is defined very widely and includes gathering, holding, analysing or using, sharing with others, moving, deleting or shredding. Particularly stringent requirements apply to processing of 'sensitive personal data' defined in the Act as information relating to: ♦ racial or ethnic origin ♦ political opinions ♦ religious or other similar beliefs ♦ trade union membership ♦ physical or mental health ♦ sexual life ♦ criminal offences or proceedings Extra care should also be taken when processing information about individuals where a duty of confidence might apply. In each case SQA's Data Protection Team can advise.
What support is available to help SQA implement this policy?	Data Protection pages within the Corporate Strategy and Governance section of the SQA Portal Information Commissioner's Office website www.ico.gov.uk

Further information

1 Processing purposes

The Act requires SQA to specify the reason(s) for processing any personal information. We need to inform the individual (usually through a privacy notice) and the Information Commissioner's Office (ICO — the regulator for Data Protection). SQA's notification to the ICO is available on the ICO website with reference Z5781759. It lists the following purposes:

- staff administration
- advertising, marketing and public relations
- accounts and records
- education
- licensing and registration
- the consideration of complaints
- crime prevention and prosecution of offenders

The ICO notification also records the types of personal data processed for each purpose; sources and disclosures; and the geographic reach of any processing. It is important that this notification fully and accurately reflects SQA's processing of personal data at a particular point in time. Any changes or additional uses of personal information should be discussed with SQA's Data Protection Team to ensure that the notification is kept up to date.

2 Obligations on SQA and its employees, appointees, nominees, agency workers and secondees

There are eight Principles included in the Act. These Principles are obligations that SQA must follow in any processing of personal information. These apply equally to SQA employees, appointees, nominees, agency workers and secondees. SQA must also ensure that any suppliers (including individual consultants) comply with these Principles in their work for SQA. The Principles are summarised below:

2.1 Personal data shall be processed fairly and lawfully, meaning:

- The processing must be generally fair and reasonable.
- Individuals must be told why SQA needs any personal information that is being gathered, including the reason for any intention to share it with others.
- They must also be told if any automated decision making will take place (eg online exams).
- The processing must not breach a confidence unless the individual has agreed, or it is required by law or it is in the greater public interest (eg whistleblowing).

- Personal information should only be accepted from sources that are lawfully allowed to supply it.
- The processing must not go beyond SQA's statutory powers.
- SQA cannot process any personal information unless one of the following conditions applies:

  — Individuals have freely given fully informed consent.

  — It is necessary for a contract with the individual or other legal obligation.

  — It will keep the individual alive.

  — It is required by a statutory obligation eg SQA's duties within the Education Act.

  — It is necessary for the legitimate interests of SQA or another, and doesn't prejudice the individual's legitimate interests.

SQA cannot process any 'sensitive personal data' unless an additional more stringent set of conditions has been satisfied. Seek advice from SQA's Data Protection Team if considering new or different processing of sensitive personal data.

2.2 Personal data shall be obtained for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose, meaning:

- Any further processing must be compatible with the original purpose for which the data was obtained.
- It must also be added to SQA's ICO notification, and consent sought from the individuals.
- Unless individuals opt-in to receiving marketing information from SQA or any other organisations, then their consent should be sought before using it for this purpose.

2.3 Personal data shall be adequate, relevant and not excessive in relation to that purpose, meaning:

- Enough personal information must be obtained to allow SQA to fulfil the purpose for gathering it (eg it must be possible to distinguish between two similar records).
- Extra items of personal information should not be collected on the basis that they might be useful for some unspecified purpose in the future.
- Where particular information is needed for a subset of individuals, but not everyone, it should only be requested for the particular subset.

2.4 Personal data shall be accurate and kept up to date, meaning:

- Reasonable steps should be taken to keep personal information up to date.
- Reasonable steps should be taken to ensure that personal information is accurate.

- Any inaccuracies (including those where the individual points out an inaccuracy) should be promptly corrected.

2.5 Personal data shall not be kept for any longer than is necessary for that purpose, meaning:

- SQA's corporate retention schedules must be consistently applied.
- Personal information must be destroyed (eg deleted or shredded) securely when it is no longer needed.

2.6 Personal data shall be processed in accordance with individuals' rights, meaning:

- SQA must ensure that its systems, processes, policies and practices are designed to accommodate individuals' option to exercise their rights.
- One important right is the individual's right to access personal information held about them. Good information management practice will ensure that all personal information about an individual can be easily located.
- Any reference to individuals in e-mails or correspondence, including any expression of opinion or intention about them, is covered by the Act. Appropriate care should be taken to express such opinions or intentions in a professional manner.

Section 5 explains individuals' rights in more detail.

2.7 Appropriate technical and organisational measures shall be taken to protect personal data, meaning:

- Personal information must be stored or sent to others in a secure manner, whether on computer or paper, internally or externally.
- The sensitivity and risk level for personal information used within a business area should be considered, and particularly stringent security controls put in place for confidential or sensitive personal information.
- SQA must ensure that its employees, appointees, nominees, agency workers and secondees using personal information (and any staff working for suppliers using personal information for which SQA is responsible) are reliable through vetting, training, monitoring or supervision.
- Colleagues and/or suppliers (including individuals) should be provided with access to personal data only as required in relation to the purpose for which it was obtained. Ensure that they are aware of their responsibilities set out in this policy and any related policies, and of the degree of access to personal information that is authorised for the purpose of their role.
- Disclose the data only to those who require it in relation to the purpose for which it was obtained. Any sharing of personal data must comply with the ICO's statutory code of practice on data sharing, which sets out mandatory requirements to ensure that data is shared in a way that is fair and in line with individuals' rights and expectations. It is important

that any requests for access to personal information from third parties are referred to SQA's Data Protection Team for advice, unless these are already covered by a partnership/ data sharing agreement.

- When disclosing personal information to the individual or anyone else, take reasonable steps to confirm their identity. Be alert to the possibility of individuals attempting to obtain personal information by deception.
- Regardless of contract value, particular requirements apply to the selection of suppliers who will use personal information on SQA's behalf (eg printers, couriers, software suppliers testing with real individual records, development consultants holding contact details for appointees). There are also specific contract terms that must be included. SQA's Procurement Team will advise.

2.8 Personal data shall not be transferred outside the European Economic Area (EEA) unless an adequate level of data protection is in place, meaning:

- A need may arise for SQA to transfer personal information outside the EEA for various reasons, eg where a supplier's equipment (such as a server) is based outside the EEA, or when exchanging information about consultants working in international markets, or information about candidates or staff based in international centres.
- The Act provides that this transfer can legitimately take place where all of the other Principles have been satisfied and either:
  - the European Commission has published a finding of adequacy for the country or territory (eg Isle of Man, Israel),

    or

  - one of a set of conditions has been satisfied (eg an individual has consented or the transfer is necessary to execute a contract with the individual or with another which is in the individual's interests),

    or

  - SQA has carried out and documented a rigorous assessment of the adequacy of data protection for the transfer to that territory.
- Advice should be sought from SQA's Data Protection Team if considering a new or different transfer of personal information outside the EEA.

3 Individuals' rights

The Act gives a number of rights to individuals and SQA must ensure that its systems, processes, policies and practices are designed to enable individuals to exercise these rights.

3.1 Right to access personal information held about them

- SQA's Data Protection Team will log and co-ordinate the response to any requests for personal information from individuals which are outside the usual run of business. The Access to Information pages of SQA's website explain the process, fee and statutory

deadline that apply to these requests. Individuals requesting access to personal information outside the usual run of business should be directed to these pages.

- Individuals may authorise a third party representative to act on their behalf when requesting their personal information. This could be a solicitor, carer or family member. In this case, SQA must be satisfied that the representative is entitled to make the request on behalf of the individual. It is the individual's responsibility to provide evidence that they have authorised the representative to make the request on their behalf. SQA's data subject access form includes a section for authorisation of third party requests.
- The right extends to include any archived information or information which has been deleted but can still be retrieved, eg held in e-mail trash.

3.2 Right to object to direct marketing

- Where an individual notifies SQA in writing that they wish to object to direct marketing, their details should be suppressed (not deleted) and no further direct marketing activity should take place.
- On receipt of such a notice, SQA's Data Protection Team should be advised to ensure that all relevant teams are made aware of the need to suppress details in any direct marketing databases.

3.3 Right to object to processing

- Individuals have a limited right to object in writing to processing which is likely to cause substantial unwarranted damage or distress in particular circumstances.
- On receipt of such a notice, SQA's Data Protection Team should be alerted to advise on the specific circumstances.

3.4 Right to object to automated decision-making

- Individuals have a limited right to object in writing to any decision-making which significantly affects them and which is solely taken by automated means.
- Where automated decision-making is planned, safeguards must be in place to protect individuals' rights in the event of a negative outcome, eg prior quality assurance or an appeal mechanism.

3.5 Right to correction

Individuals have the right to apply to the courts to have incorrect personal information rectified.

4 Compensation and other consequences

- Individuals have the right to apply to the courts for unlimited compensation for any damage they suffer through SQA's failure to comply with the Act. Where damage is suffered, they can also claim for resulting distress.

- In addition, the ICO can impose a monetary penalty on SQA up to a maximum of £500,000.
- The ICO or Procurator Fiscal can also pursue criminal prosecutions for actions by individuals that are in breach of the Act, for example:
  - passing on personal data (eg candidate results) to unauthorised persons, whether well intentioned or for financial gain
  - wilful negligence by failing to follow correct security policies or procedures when processing personal data, especially where this causes distress or damage to individuals
  - any instances of unauthorised changes or deletions to personal data that cause distress or damage to the data subject

5 Data sharing and disclosures

SQA will share personal data with partner organisations where this is necessary in relation to the purpose for which the data was obtained, and in line with its notification (eg SQA centres and the Universities and Colleges Admissions Service). Procedures are also in place to share personal data with:

- appropriate authorities where required to enable them to fulfil statutory duties, eg when necessary to prevent or detect crime or fraud, and
- researchers where required for research purposes, if relevant conditions are met

Disclosure can be unlawful even if a request comes from an individual's family member, local authority, government department or the police. It is important that correct procedures are followed so please speak to SQA's Data Protection Team for advice if you receive a third party request for personal data which is not already covered by a data sharing agreement. Any arrangements for sharing personal data must comply with the ICO's statutory code of practice on data sharing.

SQA also shares anonymised statistical data regularly with third parties. Neither the Data Protection Act nor data sharing code of practice apply to that type of sharing as long as individuals cannot be identified from the data. When sharing or publishing anonymised statistical data, SQA will ensure that it complies with the ICO's anonymisation code of practice to withhold any detailed information that could allow individuals to be identified.

6 Roles and responsibilities

6.1 Employees, appointees, nominees, agency workers and secondees

Individuals are responsible for ensuring that they understand and comply with the implications of the Act and this policy in relation to their role. They are also responsible for adhering to good information management practice.

6.2 Line managers

Line managers are responsible for ensuring that access to personal information is given to employees, appointees, nominees, agency workers and secondees in accordance with their

duties. They are also responsible for ensuring that employees, appointees, nominees, agency workers and secondees are aware of their responsibilities set out in this policy (and any related policies) and of the degree of access to personal information that is authorised for the purpose of their role. They are also responsible for reporting any actual or potential data protection breaches as described at 7 below.

6.3 SQA's Data Protection Team

SQA's Data Protection Team advises on data protection queries or issues or help in channelling more complex requests for specialist legal advice. They are also responsible for logging and collating responses to data subject access requests. The team can be contacted at data.protection@sqa.org.uk.

6.4 SQA's Senior Information Risk Officer

SQA's Senior Information Risk Officer is Maidie Cahill, Director of Corporate Services. She is responsible for leading a culture of good information management, owning policies and processes related to information risk and advising the Chief Executive on information risk.

7 Security incident reporting

If a member of staff, agency worker or secondee becomes aware of an actual or potential breach of security in relation to personal information, they should report it immediately to their line manager. They should then complete a Security Incident Report Form (available on Find a Form) and send this to information.governance@sqa.org.uk.

If an appointee or nominee becomes aware of an actual or potential breach of security in relation to personal information, it should immediately be reported to Appointee Services Manager at am@sqa.org.uk.

Quick action can be crucial in mitigating the negative effects of a breach.

8 Reporting other policy breach

If you become aware of any other type of breach of this policy, please speak to your line manager in the first instance. Line managers should then contact HR or SQA's Data Protection Team for advice.

9 Compliance

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

It is also a criminal offence for any employee, appointee, nominee, agency worker or secondee to access, use or disclose personal data without being authorised to do so for the purpose of their role. This may result in criminal prosecution.

10 Protecting personal information

SQA must continually ensure that its collection, storage and use of personal data comply with its obligations in the Data Protection Act. It is the responsibility of every member of staff, appointee, nominee, agency worker and secondee to uphold these responsibilities, treating all individuals' personal information with the same respect that they would expect for their own.

Further information on the application of the policy and practice can be obtained from SQA's Data Protection Team.

11 Glossary

The following key concepts are important in understanding this policy:

Personal data is information held about living, identifiable individuals including expressions of opinion or intention about them.

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

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

Data processor is a person or organisation who processes personal data on behalf of a data controller, eg printer, courier, software development contractor.

Data subjects are living people about whom the personal data is held.

Data subject access request is a written request from a data subject (or an authorised third party) for access to personal data about them processed by SQA.

Duty of confidence arises when SQA (the 'confidant') is provided with information by another person or organisation (the 'confider') in the expectation that the information will only be used or disclosed in accordance with the wishes of the confider.

Sensitive personal data means personal data that relates to:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership status
- physical or mental health or condition
- sexual life
- commission or alleged commission of any offence
- proceedings or sentence for any alleged offence