Processing of special category personal data and criminal offence data

Version number	2.0
Policy author	Kirsty Hurt
Policy owner	Michael Baxter
Business Area	Strategic Planning and Governance
Policy effective from	October 2023
Policy review date	October 2025 (or sooner subject to any legislative change)
Policy approved by	Executive Management Team
Policy approval date	16 October 2023
Equality impact assessment (EqIA) approval date	13 June 2022

Why do we need the policy?

This policy is a requirement under Part 4 of Schedule 1 of the Data Protection Act 2018 (the Act).

It explains SQA's procedures for complying with the data protection principles (Article 5 UK GDPR) in relation to the processing of special category personal data and criminal offence data.

Who is it for?

This policy applies to SQA employees, secondees, appointees, contractors and job applicants and anyone else whose special category personal data and criminal offence data SQA may process.

What support is available?

Contact the information governance team by email data.protection@sqa.org.uk

Introduction

The Scottish Qualifications Authority (SQA) is a public body, created under the Education (Scotland) Act 1996.

As part of our statutory and corporate functions, we process special category personal data and criminal offence data in accordance with the requirements of Article 9 and 10 of the United Kingdom General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act 2018 (DPA 2018).

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.

Special Category Personal Data

Special category data is personal data revealing:

- 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)

Criminal offence data

Criminal offence data is personal data relating to criminal convictions and offences or related security measures. This includes any personal data that is linked to criminal offences, or that is specifically used to learn something about an individual's criminal record or behaviour. It can, for example, cover the suspicion or allegations of criminal activity as well as the absence of criminal convictions.

Responsibilities

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

<u>Employees, agency workers, secondees, contractors</u>

- individuals are responsible for ensuring that they understand and comply with the requirements of data protection laws and this policy in relation to their use of special category personal data and criminal offence data

- use special category personal data and criminal offence data only in accordance with their role or contract

Data Protection Officer

SQA's Data Protection Officer is responsible for

- monitoring compliance with data protection law and with this policy in relation to the protection of special category personal data and criminal offence data

- providing advice on the use of special category personal data and criminal offence data

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

Description of data processed

SQA processes the following categories of special category and criminal offence data:

- Health or disability
- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Sexual life or sexual orientation
- Criminal offence data

SQA also processes personal data about gender reassignment. This will be treated as special category data under this policy.

We process this data about our employees, and prospective employees, to fulfil our obligations as an employer as well as for reasons of substantial public interest.

More information including the legal bases for processing this data under both Articles 6 and 9 of the UK GDPR can be found in SQA's Privacy Statement, for current employees in the SQA Employee and Secondee Privacy Statement and our Record of Processing.

Schedule 1 condition for processing

SQA processes special category personal data and criminal offence data under the following conditions of Schedule 1 of the DPA 2018:

Special category personal data

Part 1 – Conditions Relating to Employment, Health and Research, etc.

- Paragraph 1(1) employment, social security and social protection
- Paragraph 2 (1) and (2) health or social care purposes

Part 2 – Substantial Public Interest Conditions

- Paragraph 6(1) and (2)(a) statutory, etc. purposes
- Paragraph 8(1) and (2) equality of opportunity or treatment
- Paragraph 18 (1) and (2) safeguarding of children and of individuals at risk
- Paragraph 21 (1) occupational pensions
- Paragraph 24(1) and (2) disclosure to elected representatives

Criminal offence data

Part 1 – Conditions Relating to Employment, Health and Research, etc.

- Paragraph 1 employment, social security and social protection

Part 2 – Substantial Public Interest Conditions

- Paragraph (10)(a) – necessary for the purposes of the prevention of detection of an unlawful act
- Paragraph 11(1) and (2) protecting the public against dishonesty
- Paragraph (14)(a) – necessary for the purposes of preventing fraud or a particular kind of fraud
- Paragraph 33 legal claims

Part 3 – Additional Conditions Relating to Criminal Convictions, etc.

- Paragraph 36 extension of conditions in Part 2 of Schedule 1 referring to substantial public interest.

SQA may process personal data relating to criminal convictions as part of recruitment and employment checks to protect the public against dishonesty.

The Data Protection Principles

The principles set out in Article 5 of the UK GDPR require personal data to be:

1. processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
2. collected for specified, explicit and legitimate purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation)
3. adequate, relevant and not excessive in relation to the purposes for which they are processed (data minimisation)
4. accurate and where necessary kept up to date (accuracy)
5. kept in a form which permits identification for no longer than is necessary for the purposes for which the data are processed (storage limitation)
6. processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical and organisational measures (integrity and confidentiality).

How SQA meets the Data Protection Principles

Lawful fair and transparent

SQA provides clear and transparent information to individuals about why we process their personal data, including our lawful basis, in our privacy statements. Depending on the circumstances, this information can be provided through just in time statements and verbally where appropriate.

SQA processes special category personal data and criminal offence data for the substantial public interest conditions outlined in this policy and to meet the requirements placed on SQA as a public body such as by the Equality Act (2010).

Our processing for the purposes of employment relates to our obligations as an employer.

Purpose limitation

SQA processes special category personal data and criminal offence data for the following purposes:

- equal opportunities monitoring
- recruitment and secondment purposes, such as assessing an applicant or secondee's suitability for a role and undertaking enhanced background or security checks (Disclosure Scotland and CTC) where they are required by the nature of the role. This includes both internal and external recruitment and secondment and where necessary involves the sharing of data. More information about this can be found in SQA's Privacy Statement, for current employees in the SQA Employee and Secondee Privacy Statement and our Record of Processing.
- supporting reasonable adjustments and special arrangements for staff
- supporting trans staff
- supporting reasonable adjustments and assessment arrangement for candidates
- supporting post results and alternative evidence review requests for candidates
- supporting alternative exam venue and co-incident exam requests for candidates
- carrying out investigations including where these relate to grievances, malpractice and complaints, and staff disciplinary/dismissal proceedings
- management of staff absences, including sickness and maternity/paternity leave
- provision of human resources and occupational health services
- facilitating staff enrolment in an occupational pension scheme
- complying with health and safety obligations including reporting of accidents
- deduction of Trade Union subscriptions directly from an employee's salary where this is requested
- sharing information with relevant agencies in relation to children and adults at risk, preventing fraud and/or disclosing information to an anti-fraud organisation
- preventing or detecting crime and/or disclosing information to the police or other law enforcement agencies
- assisting elected representatives such as MSPs, MPs and local government councillors with requests for assistance on behalf of their constituents

These purposes are detailed in SQA's privacy statements.

Processing will be restricted to only what is necessary for the relevant purpose. If it is considered that processing for a further purpose is required, and that processing is not

based on consent, we will decide whether it is compatible with the original purpose. The data will not be used in a way that is incompatible with the original purpose for which it was collected.

Data minimisation
We only collect the special category personal data or criminal offence data that is necessary for and proportionate to our purposes. For example, where data is needed for a subset of individuals, it will be requested only for that subset.

SQA's data protection training, policy and associated guidance make clear that only the data needed for a particular purpose should be collected, whilst forms and other tools used for data collection are designed with data minimisation in mind.

Accuracy
SQA will ensure as far as possible that the data we process is accurate and kept up to date. We will take necessary steps to rectify, replace or erase any inaccurate data when it is identified. Unless we cannot do so due to the lawful basis upon which we process that data, or where it is not currently possible due to technical limitations. Where this is the case, an addition will be made to that personal data noting the inaccuracy.

Staff are made aware of the need to ensure the accuracy of data and interfaces are provided for them to keep their own personal data up to date.

Storage Limitation
SQA's retention schedule sets out the length of time that records, including those that contain special category personal data and criminal offence data, need to be kept. Retention periods set out in this are based on SQA's business needs and where applicable, legal and/or regulatory obligations.

The retention schedule must be consistently applied to ensure that personal data is securely destroyed when it is no longer needed. It is reviewed annually and updated when necessary.

Security
SQA has a range of technical and organisational security measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, or damage. These measures are proportionate to the risk associated with the processing.

The technical measures include the following:

- encryption
- firewalls
- anti-virus software,
- vulnerability scanning and penetration testing
- user authentication
- role based and password-controlled access

The organisational measures include the following:

- ensuring all employees complete data protection and information security training at induction and at regular intervals to remind them of their responsibilities

- exercising due diligence in the recruitment or engagement of employees, appointees, contractors, suppliers and others to ensure their reliability
- physically securing and managing access to SQA buildings
- implementing and communicating policies and guidance to support compliance with legislation and good practice.

Accountability
SQA has put in place a number of measures to meet and demonstrate our compliance with the accountability requirement. These include:

- appointment of a Data Protection Officer who reports into the highest level of management.
- maintaining documentation of our processing activities including the Record of Processing which sets out the personal data categories we process, the purposes, the lawful basis, our retention periods for the data and our privacy statements which explain to individuals how and why we process their personal data.
- entering into written agreements with controllers and/or processors where we share data with them.
- undertaking data protection impact assessments (DPIA) for any new or changed use of personal data and in particular, where that use is likely to result in a risk to individuals' data protection rights and freedoms.

Retention and disposal policies

Our retention and disposal practices are set out in our Retention and Disposal Policy and SQA's Retention Schedule. Retention periods for personal data are also included in our Record of Processing.

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.

- Data Protection Policy
- Information Security Policy
- Records Management Policy
- Retention and Disposal Policy

The following documents are also relevant.

- Record of Processing
- Security Incident Management Procedure
- 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)