PRIVACY AND DATA PROTECTION POLICY

1. Purpose

It is the policy of Scottish Quality Crops (SQC) to manage data in line with all current data protection legislation.

2. Scope

This Policy is applicable to all SQC employees, directors and contractors, regardless of location or job function.

This policy is communicated to all employees, directors and contractors as part of their SQC induction programme and when revisions are published.

This Policy is also applicable to relevant committees, external bodies or individuals acting on behalf of SQC.

3. Terms and Definitions

Availability	Authorised users should be able to access the data if they need it for authorised purposes.
Confidentiality	Only people who are authorised to use the data can access it.
Integrity	Personal data should be accurate and suitable for the purpose for which it is processed.
Personal data	Data (stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).
Processing	Any activity that involves the use of personal data. It includes obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.
Sensitive personal data	includes personal data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions. Sensitive personal data can only be processed under strict conditions, including with the consent of the individual.

4. Policy Wording

4.1. Policy Statement

SQC receives, uses and stores personal information from its certified clients, partner organisations, government and contractors and SQC employees and directors. It is important that this information is handled lawfully and appropriately in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

4.2 About this Policy

This policy, and any other documents referred to in it, sets out the basis on which we will process any personal data that we collect or process.

This policy does not form part of any employee's contract of employment and may be amended at any time.

We have a separate contract in place with the Certification Body who process personal data on our behalf.

The SQC Managing Director is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the SQC Managing Director.

4.3 Data Protection Principles

Anyone processing personal data, must ensure that data is:

- Processed fairly, lawfully and in a transparent manner *
- Collected for the specified, explicit and legitimate purposes in Schedule 1, and any further processing is completed for a compatible purpose
- Adequate, relevant and limited to what is necessary for the intended purposes
- Accurate, and where necessary, kept up to date
- Kept in a form which permits identification for no longer than necessary for the intended purposes
- Processed in line with the individual's rights and 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
- Not transferred to people or organisations situated in countries without adequate protection

* Fair and Lawful Processing - the Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the Data Protection Requirements, we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): when the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. We do not receive or process sensitive personal data, but should this occur, we will ensure that additional conditions specified under Data Protection Requirements are met.

4.4 Processing for Limited Purposes

In the course of our business, we may collect and process the personal data set out in Schedule 1. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including our Certification Body, business partners, contractors in technical, payment and delivery of services, and others).

We will only process personal data for the specific purposes set out in Schedule 1 or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject at the time of collecting the data.

4.5 Notifying Individuals

We usually collect data in the normal course of our business for business purposes, from our business contacts, but if we collect personal data directly from an individual (employees for example), we will inform them about:

i. The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
ii. Where we rely upon the legitimate interests of our business to process personal data, the legitimate interests pursued.
iii. The types of third parties, if any, with which we will share or disclose that personal data.
iv. Whether or not SQC intends to transfer personal data to a non-European Economic Area (EEA) country or international organisation and the appropriate and suitable safeguards in place.
v. How individuals can limit our use and disclosure of their personal data.
vi. Information about the period that their information will be stored or the criteria used to determine that period.
vii. Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing as provided in the Data Protection Requirements.
viii. Their right to object to processing and their right to data portability.

ix. Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
x. The right to lodge a complaint with the Information Commissioners Office.
xi. Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
xii. Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
xiii. Whether or not we utilise automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

We will also inform data subjects whose personal data we process that SQC is the data controller with regard to that data, and our contact details are SQC, The Rural Centre, West Mains, Ingliston, EH28 8NZ and the person responsible for Data Protection Compliance is the Managing Director.

4.6 Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

4.7 Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

4.8 Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

4.9 Processing in line with Data Subject's Rights

We will process all personal data in line with data subjects' rights, in particular their right to:

i. Confirmation as to whether or not personal data concerning the individual is being processed.
ii. Request access to any data held about them by a data controller (see also Clause 4.11 Subject Access Requests).
iii. Request rectification, erasure or restriction on processing of their personal data.
iv. Lodge a complaint with a supervisory authority.

v. Data portability.
vi. Object to processing including for direct marketing.
vii. Not be subject to automated decision making including profiling in certain circumstances.

4.10 Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if that processor agrees to comply with those procedures and policies by way of a data sharing agreement, or puts in place adequate security measures.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data (see explanations under Section 3 – Terms and Definitions).

Security procedures include:

Secure lockable desks and cupboards	Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential)
Employee laptops	Laptops should be password secured (and logged off) before leaving the laptop unattended.
Data minimisation	The principle that states that data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy.
Pseudonymisation and encryption of data	When appropriate and if they hold confidential information of any kind.
Methods of disposal	Paper documents should be shredded or equivalent. Digital storage devices should be physically destroyed or professionally cleared of data when they are no longer required.
Equipment	Individual monitors must not show confidential information to passers-by.

We may transfer any personal data we hold to a country outside the EEA or to an international organisation, provided that one of the following conditions applies:

i. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
ii. The data subject has given consent.

iii. The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

iv. The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

v. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

In the event of a personal data breach, the SQC Managing Director shall record the incident and where necessary, report it to the individual – in accordance with UK GDPR.

4.11 Subject Access Requests

Individuals must make a formal request in writing for information we hold about them to the SQC Managing Director.

Where a request is made electronically, data will be provided electronically where possible.

4.12 Changes to this Policy

SQC will review this policy on an annual basis. SQC reserves the right to change this policy at any time. Where appropriate, we will notify changes by mail or email.

SQC Data Protection Policy Schedule 1

Data That We Collect and Process

1. We hold contact information including postal addresses, e-mail addresses, and phone numbers of members, partners, suppliers and contractors
2. With respect to suppliers and contractors, we hold bank account details to enable us to make payments.
3. We hold additional personal information about SQC employees and directors, which we detail in a separate policy statement that is provided to them. We do not hold sensitive personal data.

Purposes for Which Data is Held and Processed

1. For Legitimate Business Reasons
2. SQC works in collaboration with stakeholder organisations, public sector bodies, and other business clients and individuals. We exchange with them, information and reports on the purpose, method, progress, finances and outcomes of our work. Our data processing is usually on a basis of business to business.
3. To fulfil Contractual and Statutory Obligations – We have contractual obligations to our Certification Body, suppliers, contractors, directors and employees. We have statutory obligations to HMRC and Government agencies.