Data Security Policy

Contents

1. Introduction

QRS recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, QRS will facilitate the secure and uninterrupted flow of information, both within the company and in external communications. QRS believes that security is an integral part of the information sharing process and the policies outlined below are intended to support information security measures throughout the company.

QRS is registered with the ICO, registration number Z4975915.

2. Definition

For the purposes of this document, information security is defined as the preservation of: confidentiality: protecting information from unauthorised access and disclosure; integrity: safeguarding the accuracy and completeness of information and processing methods; and availability: ensuring that information and associated services are available to authorised users when required.

Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

3. Protection of Personal Data

This policy applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. In the course of our business we may process sensitive personal data which includes; ethnicity, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

QRS holds and processes information about employees, customer databases, research participants and other data sources for commercial purposes. When handling such information, QRS, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the UK General Data Protection Regulation/Data Protection Act.

The Company's QMS and ISMS functions in accordance with the ISO20252:2019 and ISO 27001:2017 standards and all legal, regulatory, and statutory requirements as identified below:

- The Data Protection Act (2018)
- General Data Protection Regulation (EU) 2016/679
- The Freedom of Information Act (2000)

- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications Regulations (2003)

4. Information Security Responsibilities

QRS believes that information security is the responsibility of all members of staff. Every person handling information, personal data, or using QRS information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at QRS. Staff responsibilities are included in their contracts of employment.

This Policy is the responsibility of the Board of Director's; supervision of the Policy will be undertaken by the Board.

5. Compliance with Legal and Contractual Requirements

QRS IT facilities must only be used for authorised purposes. QRS may from time to time monitor or investigate usage of IT facilities and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings.

5.1 Monitoring of Operational Logs

QRS shall only permit the inspection and monitoring of operational logs by computer operations personnel and system administrators. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur (i) when required by and consistent with law; (ii) when there is reason to believe that a violation of law or of a QRS policy has taken place; or (iii) when there are compelling circumstances.

Access to QRS personal data in general and the privacy of users' files will be respected but QRS reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with QRS policies and regulations, and to determine which records are essential for QRS to function administratively or to meet its obligations. Except in emergency circumstances, authorisation for access must be obtained from a Director, and shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

5.2 Protection of Software

To ensure that all software and licensed products used within QRS comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, QRS will carry out checks from time to time to ensure that only authorised products are being used, and will keep a record of the results of

those audits. Unauthorised copying of software or use of unauthorised products by staff may be grounds for disciplinary, and where appropriate, legal proceedings.

5.3 Virus Control

QRS will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of QRS computers, including laptops, need to ensure that up-to-date virus protection is maintained on their machines.

6. Retention and Disposal of Information

All staff have a responsibility to consider security when disposing of information in the course of their work. Retention periods for research records are:

- Primary records: **12 months (unless explicit consent has been obtained otherwise).**
- A copy of all other final versions of documents related to the research project: **24 months.**

If the research is later repeated, or further research is later carried out in the same project, the storage period shall be said to begin upon conclusion of the entire research project.

Retention periods for employment records and financial information will be 7 years.

7. Reporting

All staff should report immediately to a Director, any observed or suspected security incidents where a breach of QRS's security policies has occurred, any security weaknesses in, or threats to, systems or services. Please see our Data Breach Policy for further details.

Software malfunctions should be reported to the IT department / Lee Tomlin (Director)

8. Business Continuity

QRS will implement, and regularly update, a business continuity management process to counteract interruptions to normal QRS activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

Not relevant for clients/customers

These policies supplement your terms of employment but are not of contractual effect. Their purpose is to explain the Company's current policies and procedures but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.

Data Protection Policy

1. Introduction

QRS holds and processes information about employees, customer databases and other data subjects for commercial purposes. When handling such information, QRS, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the General Data Protection Regulation/Data Protection Act. In summary these state that personal data shall be:

- ⇨ Processed lawfully, fairly and in a transparent manner in relation to individuals;
- ⇨ Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- ⇨ Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- ⇨ Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- ⇨ 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- ⇨ 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.
- ⇨ Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.

The Company's QMS and ISMS functions in accordance with the ISO20252:2019 and ISO 27001:2017 standards and all legal, regulatory, and statutory requirements as identified below:

- The Data Protection Act (2018)
- General Data Protection Regulation (EU) 2016/679
- The Freedom of Information Act (2000)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)

- Privacy and Electronic Communications Regulations (2003)

2. Definitions

"Staff" and "other data subjects" - may include past, present and potential members of those groups.

"Other data subjects" and "third parties" - may include contractors, suppliers, contacts, referees, friends or family members.

"Processing" refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information.

3. Notification of Data Held

QRS shall notify all staff and other relevant data subjects of the types of data held and processed by QRS concerning them, and the reasons for which it is processed.

4. Staff Responsibilities

All staff shall:

- ⇨ Ensure that all personal information which they provide to QRS in connection with their employment is accurate and up-to-date;
- ⇨ Inform QRS of any changes to information, for example, changes of address;
- ⇨ Check the information which QRS shall make available from time to time, in written or automated form, and inform QRS of any errors or, where appropriate, follow procedures for updating entries on computer forms. QRS shall not be held responsible for errors of which it has not been informed.

Staff shall ensure that:

- ⇨ All personal information is kept securely.
- ⇨ Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party.
- ⇨ Unauthorised disclosure may be a disciplinary matter and may be considered gross misconduct in some cases.
- ⇨ Notify the relevant line manager and/or DPO should it come to light that personal data requires updating or has been kept longer than our retention policy (see Data Security Policy above).

5. Subject Consent

In some cases, such as the handling of personal and/or sensitive information, QRS is entitled to process such data only with the consent of the individual.

6. Sensitive Information

QRS may process sensitive information regarding an individuals' ethnicity, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences. For example, some projects will bring employees into contact with children (including young people under the age of 16), and/or Government research projects, and QRS has a duty under the relevant Acts of Law, other enactments and contractual agreements, to ensure that staff are suitable for the job. QRS may also require such information for the administration of the sick pay policy, the absence policy or the equal opportunities policy, for assessment.

7. The Data Controller and the Designated Data Controllers

QRS is the data controller under the Act (unless acting as a Data Processor under client contract), and the Board of Directors is ultimately responsible for implementation. Responsibility for day-to-day matters will be delegated to data and project managers.

8. Retention of Data

QRS will keep different types of information for differing lengths of time, depending on legal and operational requirements. Please refer to our Data Security Policy.

9. Compliance

Compliance with GDPR/The Act is the responsibility of all members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings. Staff should refer to their contracts of employment in conjunction with our Clear Desk Policies, Confidentiality Policy, Data Security Policy, Information Security Policy, Password Policy and Use of Company Facilities Policy.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the IT Director.

Any individual who considers that the policy has not been followed in respect of their personal data, should raise the matter with the Data Protection Officer.

Members of the public should refer to our Privacy Policy for further information www.qrs-research.co.uk/privacy-policy

Staff should refer to our grievance procedures should the matter not be resolved.

These policies supplement your terms of employment but are not of contractual effect. Their purpose is to explain the Company's current policies and procedures but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.