



## **DATA SECURITY POLICY**

### **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.

This policy is based on recommendations contained in British Standard 7799 - A Code of Practice for Information Security Management.

### **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

### **Protection of Personal Data**

QRS holds and processes information about employees, customer data bases 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 Data Protection Act 1998 (the 1998 Act).

### **Information Security Responsibilities**

Qrs believes that information security is the responsibility of all members of staff. Every person handling information 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.

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

## **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.

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 Records in general, 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 teaching 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

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.

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.

## **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 are:

- Primary records: **12 months**
- 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.

## **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.

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

**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.

*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

### Introduction

QRS holds and processes information about employees, customer data bases 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 Data Protection Act 1998 (the Act). In summary these state that personal data shall:

1. be processed fairly and lawfully,
2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose,
3. be adequate, relevant and not excessive for the purpose
4. be accurate and up-to-date,
5. not be kept for longer than necessary for the purpose,
6. be processed in accordance with the data subject's rights,
7. be kept safe from unauthorised processing, and accidental loss, damage or destruction,
8. 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.

### 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.

### Notification of Data Held

QRS shall notify all staff and students 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.

### 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 up-dating 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.

- 

## **5. Rights to Access Information**

5.1 Staff, students and other data subjects in the University have the right to access any personal data that is being kept about them either on computer or in structured and accessible manual files. Any person may exercise this right by submitting a request in writing to the Information Security Officer.

5.2 The University will make a charge of £10 for each official Subject Access Request under the Act.

5.3 The University aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing by the Information Security Officer to the data subject making the request.

## **Subject Consent**

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

## **Sensitive Information**

The QRS may process sensitive information about a person's health, disabilities, criminal convictions, race or ethnic origin. For example, some projects will bring employees into contact with children, including young people between under the age of 16, and QRS has a duty under the Children Act 1989 and other enactments 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.

## **The Data Controller and the Designated Data Controllers**

QRS is the data controller under the Act, and the Board of Directors is ultimately responsible for implementation. Responsibility for day-to-day matters will be delegated to project managers as designated data controllers.

## **Retention of Data**

QRS will keep different types of information for differing lengths of time, depending on legal and operational requirements.

## **Compliance**

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

Any individual, who considers that the policy has not been followed in respect of personal data about him- or herself, should raise the matter with a Director. If the matter is not resolved it should be referred to the staff grievance procedure.

*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.*