1. Objectives, Aim and Scope

1.1. Objectives

The objectives of RCU Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

1.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by RCU by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.
- Giving our customers full confidence that we will support them in the implementation of their own information security policies and procedures
- Complying fully with contractual requirements to protect sensitive and confidential client information

1.3. Commitment to Continual Improvement

RCU is committed to continual improvement of the Information Security Management System and will establish processes to ensure that continual improvement takes place and a culture that encourages continual improvement at all levels.

1.4. Scope

This policy applies to all information, information systems, networks, applications and locations.

The organisation and its context are described in Annex A.
Interested parties relevant to information security and the interfaces and dependencies between RCU and interested parties are described in Annex B.

2. Responsibilities for Information Security

2.1. Ultimate responsibility for information security rests with the Managing Director of RCU, but on a day-to-day basis the Deputy Director shall be responsible for managing and implementing the policy and related procedures.

2.2. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

2.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

2.4. The Information Security Policy shall be approved, reviewed and updated by the RCU Board. This review shall take place annually.

2.5. Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

2.6. Each member of staff shall be responsible for the operational security of the information systems they use.

2.7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

2.8. Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

2.9. Supplier Security Policy

- RCU will carry out an initial risk assessments for all new suppliers and will identify if a Compliance an Information Security Risk Assessment is required.
- Information Security Group on an annual basis or earlier if a need is identified will monitor and review risks associated with each supplier.
- All suppliers will be given appropriate Information Security awareness training.
- The Appendix lists the responsibility and access rights of ICT suppliers

3. Legislation

3.1. The RCU is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the RCU, who may be held personally accountable for any breaches of information security for which they may be held responsible. The RCUshall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000(in particular as it applies to our public sector clients)
- Health & Social Care Act 2001
- The Single Equality Act 2009

4. Policy Framework

4.1. Management of Security

- At Board level, responsibility for Information Security shall reside with the Managing Director.
- The Deputy Director shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.
- The Information Security Group, chaired by the Deputy Director, shall meet at least 4 times a year. The Group will formally establish an Information Security Objective Plan which will list the objectives for the year, the timescale for implementation, where appropriate measurable outcomes and the person responsible for each objective. The plan will be reviewed at each meeting, progress monitored and where appropriate updated. Achievement of Security Objectives will be reported annually to the Board.
- The Information Security Group will monitor, analyse and evaluate the effectiveness of current information security procedures and practices. The Group will receive relevant management reports and measurements (including an analysis of security risks and actions) and will assess changes in the external environment. Membership of the Information Security Group will include all staff. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed. Management review activities carried out by the Information Security Group will include:
    - Status of actions from previous management reviews
    - Progress with current Information Security Objectives
    - Potential impact of internal and external changes
    - Feedback from interested parties
    - Results from risk assessment and risk treatment plans
    - Future Information Security Group Objectives

Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.
- As and when judged necessary, RCU will seek expert advice from suitably qualified individuals and organisations to ensure the effectiveness of its procedures.

4.2. Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and information security expectations of staff shall be included within the staff handbook.

4.3. Access Controls Policy

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

The ISMS Staff Responsibilities and Training Matrix will record role based authorised access on an individual basis. The matrix will be continually updated and maintained to reflect accurate records of access.

4.4. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

4.5. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

4.6. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

4.7. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

4.8. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Managing Director.

4.9. Information Security Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of the severity of impact and the likelihood of occurrence.At weekly staff meetings (attended by all staff) new risks will be discussed, assessed and recorded in the risk assessment plan (S8) and appropriate risk treatments identified. Previous actions recorded in the risk assessment plan will be reviewed and monitored. All risks shall have a named person who shall be responsible for the management of that risk.

Project Managers shall have a formal record of risk assessments relating to their project. The project type (established when a project is set up) will determine whether a new risk assessment needs to be created or an existing one reviewed and where appropriate updated. Staff shall carry out risks assessments for any new systems or processes that are not set up as a formal project. Actions resulting from the risk assessment shall be recorded in the company risk assessment plan (S8).

4.10. Information security events and weaknesses

Information security incidents and suspected weaknesses are to be reported through the RCU Quality System R25 form. This will identify the nature of the incident and initial actions to taken. All potential information security events shall be reported to the Director or nominee and investigated to establish their cause and impacts with a view to avoiding similar events and appropriate actions put in place. RCU will maintain a register of all information security events and this will be reviewed by the Information Security Group.

4.11. Classification of Sensitive Information.

RCU will implement appropriate information classifications controls, based upon the results of formal risk assessment.

The classification **RCU Confidential** – shall be used for all personal information and records.

The classification **RCU Restricted -** shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the RCU or its officers or cause substantial distress to individuals;
- adversely affect the reputation of clients or its officers or cause distress to individuals in that organisation;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

4.12. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Details of the procedures are outlined in the ICT Operating Policy and Guidelines.

4.13. User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, should only be used in accordance with agreed procedures.Details of the procedures are outlined in the ICT Operating Policy and Guidelines.

4.14. Transfer Data

Electronic data should only be transferred according to agreed procedures. Failure to comply with this may be lead to disciplinary action. Details of the procedures are outlined in the ICT Operating Policy and Guidelines.

4.15. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan before they commence operation.

4.16. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Deputy Director.

4.17. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Senior Data Analyst. Users shall not install software on the organisation's property without permission from theDeputy Director. Users breaching this requirement may be subject to disciplinary action.

4.18. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

4.19. Reporting

The Deputy Director shall keep theManaging Director andRCU Board informed of the information security status of the organisation by means of regular reports and presentations.

4.20. Policy Audit

This policy shall be subject to audit by February 2016.

4.21. Further Information

Further information and advice on this policy can be obtained from Graham Whalley on 01772 734855.

5. Policy approved by:

____
Signature: [Richard Boniface, Director, RCU on behalf of the RCU Board]

Issue
Last amended: October 2016
Board Approval October 2016
Member staff responsible for implementing the regulations: Richard Boniface