Data Classification Policy & Procedure

QRS generates and holds a wide variety of information that must be protected against unauthorised access, disclosure, modification, or other misuse. Efficient management of such assets is also necessary to comply with legal and regulatory obligations such as relevant Data Protection legislation, and to ensure efficient handling of Freedom of Information requests. Different types of information require different protection measures and therefore, applying classification markings of information assets is vital to ensuring effective information security and management.

Purpose

- ⇨ This Data Classification Policy together with the accompanying technical marking controls are intended to help staff determine what information can be disclosed to external parties, as well as the relative sensitivity of information that should not be disclosed outside of QRS without proper authorisation.
- ⇨ This policy also helps to ensure that correct classification and handling methods are applied to their day to day activities and managed accordingly.
- ⇨ QRS information assets should only be made available to all those who have a legitimate need to access them.
- ⇨ The integrity of information must be maintained; information must be accurate, complete, timely and consistent with other related information and events.

Scope

- ⇨ This policy guidance covers information that is either stored or shared via any means including those created prior to the publishing of this policy. This includes: electronic information, information on paper and information shared orally or visually (such as telephone and video conferencing).
- ⇨ Where QRS holds information on behalf of another organisation with its own classification system, an agreement shall be reached as to which set of technical controls and handling guidelines shall apply.

Definitions

Information Administrator:	An individual who is responsible for the maintenance and protection of the information.
Information Asset:	A body of information which is organised and managed as a single entity and value for QRS.
Information Asset Owner:	All information assets shall be “owned” by a head of department and/or a named individual within QRS. They will have final responsibility of data protection and would be held liable for any negligence when it comes to protecting QRS’s information assets.

Responsibilities

The IT Director and/or Data Protection Officer are responsible for:

- ⇨ Approving the Information Classification system, associated data management policies and any subsequent changes to these.
- ⇨ Publicising the classification system and data management policies for electronically stored information and
- ⇨ Providing appropriate IT facilities/mechanisms to facilitate compliance with this policy for centrally maintained information.

Information Asset Owners are responsible for:

- ⇨ Identifying the appropriate information classification level for any information within their care.
- ⇨ Ensuring that the appropriate management policies about storage, publishing, disposal etc. are followed.
- ⇨ Ensuring that information is processed and managed in accordance with QRS policies including but not limited to the Information Security Policy, Data Security Policy, Confidentiality Policy, Data Breach Policy and Data Protection Policy.

All members of QRS (including staff, contractors, agency workers and associates) are responsible for

- ⇨ Handling information in accordance to their classification.
- ⇨ Complying with this policy and with relevant legislation.

Policy

There are 4 levels of classification

Business Confidential:	This definition covers sensitive business information. Typical examples are proposals, quotations, and correspondence containing pricing details or financial information; this category does not normally include personal information
Staff Confidential:	This definition covers QRS full time staff and freelancers. Typical examples are internal management records, technical and project documentation, and general HR records
Participant Confidential:	Personal information relating to participants, including data files, sample files, completed questionnaires
Public	Available to any member of the public without restriction.

- ⇨ All information held by or on behalf of QRS will be categorised according to the Information Classification above.
- ⇨ Classification labels will show in the following locations for files/documents:
  - Word – In the footer of the document in the left-hand corner and the status bar at the bottom of the screen.
  - Excel – Status bar at the bottom of the screen.
  - Power Point – Status bar at the bottom of the screen.
  - Email – Classification labels are currently not applied to emails. Refer to 'use of companies facilities policy' for further information of the company's email policy.
- ⇨ QRS classification policy would be mapped to clients' files/documents as and when required.
- ⇨ The Information Asset Owner will assess the value, sensitivity and the risk of confidentiality breach to their data set. Once the classification has been established any documents containing this information must be systematically marked as such.
- ⇨ Any information which is not explicitly classified will be classified as confidential, pending classification, by default to avoid data leakage. Questions about the proper classification of a specific piece of information or a dataset should be addressed to your manager. Where there is a mix of information from different classification levels, the more secure level should be adopted.
- ⇨ All information must be secured to meet the requirements of their respective classification levels as above.
- ⇨ Where a third party will be responsible for handling the information on behalf of QRS, the third party shall be required to adhere to this policy prior to the sharing of information.

- ⇨ Where information is discovered to have been incorrectly classified, or not to have been managed in accordance with its Information Classification, this should be reported immediately to the IT Director who will log the incident and advise of the appropriate action to be taken.

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.