DATA BREACH POLICY

1.0 Introduction

1.1 QRS Market Research Ltd ("The Company") holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

2.0 Purpose

2.1 The Company is obliged under the General Data Protection Regulation [GDPR] to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the business.

3.0 Scope

3.1 This Policy relates to all personal and sensitive data held by The Company regardless of format.

3.2 This Policy applies to all employers, employees and workers at The Company. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of The Company.

3.3 The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4.0 Definition / Types of Breach

4.1 For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

4.2 An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to The Company's information assets and/or reputation.

4.3 An incident includes but is not restricted to, the following:

a) Loss or theft of confidential or sensitive data or equipment on which such data is stored
b) Equipment theft or failure (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record).
c) Unauthorised use of, access to or modification of data or information systems attempts (failed or successful) to gain unauthorised access to information or IT system(s).
d) Unauthorised disclosure of sensitive / confidential data Website defacement.
e) Hacking attack
f) Unforeseen circumstances such as a fire or flood Human error
g) 'Blagging' offences where information is obtained by deceiving the organisation who holds it

5.0 Reporting an incident

5.1 Any individual who accesses, uses or manages The Company's information is responsible for reporting data breach and information security incidents **immediately** to the Data Protection Officer by email (dpo@qrs-research.co.uk) and phone (01707 331 332) and also notify the Director responsible for IT by email (lee@qrs-research.co.uk).

5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable taking into account that time is of the essence.

5.3 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. See Appendix 1

5.4 All staff should be aware that any breach of the Data Protection Act/GDPR may result in The Company's Disciplinary Procedures being instigated.

6.0 Containment and Recovery

6.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

6.2 An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the DPO).

6.3 The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

6.4 The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

6.5 Advice from 3rd party experts (e.g. IT or Legal) may be sought in resolving the incident promptly.

6.6 The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

7.0 Investigation and Risk Assessment

7.1 An investigation will be undertaken by the LIO immediately and wherever possible within 24 hours of the breach being discovered / reported.

7.2 The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

7.3 The investigation will need to take into account the following:

- The type of data involved and its sensitivity.
- The protections that are in place (e.g. encryptions).
- What's happened to the data, has it been lost or stolen.
- Whether the data could be put to any illegal or inappropriate use.
- Who the individuals are, number of individuals involved and the potential effects on those data subject(s).
- Whether there are wider consequences to the breach.

8.0 Notification

8.1 The LIO and / or the DPO, in consultation with the Director of IT will determine who needs to be notified of the breach.

8.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements.
- Whether the breach has involved client's customer data which in turn would require their own investigation.
- Whether the breach has involved encrypted or unencrypted personal data.
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Would notification help The Company meet its obligations under the seventh data protection principle;
- If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data and/or sensitive personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/for-organisations/report-a-breach/
- The dangers of over notifying will be taken into account. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

8.3 Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact The Company for further information or to ask questions on what has occurred.

8.4 The LIO and or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.5 The LIO and or the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

8.6 All actions will be recorded by the DPO.

9.0 Evaluation and response

9.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

9.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

9.3 The review will consider:

- Where and how personal data is held and where and how it is stored.
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure; sharing minimum amount of data necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

9.4 If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the Board.

APPENDIX 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of Department immediately, complete Section 1 of this form and email it to the Data Protection Officer dpo@qrs-research.co.uk and Head of IT lee.tomlin@qrs-research.co.uk where appropriate

Section 1: Notification of Data Security Breach	**To be completed by Head of Dept or person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	**To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach and if appropriate IT where applicable**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto the central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Company or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data **Sensitive personal data** (as defined in the Data Protection Act) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; Personal information relating to vulnerable adults and children; Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; Security information that would compromise the safety of individuals if disclosed. **Data Protection Officer and/or Lead Investigation Officer** to consider whether it should be escalated to the Board	

Section 3: Action taken	**To be completed by Data Protection Officer and/or Lead Investigation Officer**
Incident Number	e.g. year/001
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Data Protection Office and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer and/or Lead Officer:	
Notification to ICO	**Yes/No If YES, notified on:** **Details:**
Notification to data subjects	**Yes/No If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**Yes/No If YES, notified on:** **Details:**