Breach and GDPR Rights Policy

Version 1

Introduction & Description - This policy defines the process for reporting a breach of personal data, subject access requests and how Rowley Clinical Neuropsychology Services Ltd will ensure the individual rights as established in the General Data Protection Regulations.

1. Definitions

For the purpose of this policy the following definitions apply:

- **RCNS Ltd** means Rowley Clinical Neuropsychology Services Ltd. Any reference to RCNS Ltd within this policy refers to the legally established company of Rowley Clinical Neuropsychology Services Ltd, which is listed with Companies House under reference 13832672.
- **Company head office** means RCNS Ltd, C/O Taxevo 1 Cedar Office Park, Cobham Road, Ferndown Industrial Estate, Wimborne, England, BH21 7SB.
- **Associates** means qualified clinical psychologists who provide psychology services on the case that are legally separate trading entities (either self-employed sole traders or limited companies) that are appointed by RCNS Ltd to provide psychology services.
- **Data subject** means an individual who is the subject of personal data. In other words, the data subject is the individual whom particular personal data is about.
- **Data controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed.
- **Data processor** in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
- **Processing** in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.
- **Information Commissioners Office –** the ICO is the UK regulatory authority and the agency responsible for information privacy and legislation in the UK.
- **Individual rights** mean the 8 rights for individuals as set out in the GDPR.

2. Definition of a Breach of Data Protection

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever the following occur:

- Any personal data is lost, destroyed, corrupted or disclosed
- If someone accesses the data or passes it on without proper authorisation
- If the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Some more specific examples of data breaches may be described as follows, however this list is not exhaustive:

- Access by an unauthorised third party
- Deliberate or accidental action by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Any incident that involves the actual or potential loss, disclosure or any other security incident relating to personal and sensitive information shared with RCNS Ltd must be investigated to determine whether a breach of personal data has occurred.

3. Investigation

Where an incident occurs that may have the potential to constitute a personal data breach this incident must be reported to a senior manager and will in all instances be fully investigated by the data protection officer.

All potential incidents reported to the data protection officer will be recorded permanently and may be referred to in future investigations.

The data protection officer will be given full access to the facts and all information relating to the incident. The data protection office may collect the following information during the course of the investigation:

- A formal interview with the associated individuals
- Written statements
- Copies of emails
- Physical inspection of workspace and any IT hardware involved
- Previous incident reports/investigations

Actions taken by the data protection officer to investigate the potential incident will not be limited to the points above. All necessary steps will be taken to provide a comprehensive overview of the incident.

Where evidence suggests that a breach of personal data has occurred, the records will reflect that a breach of data protection has occurred, and a formal report will be produced. As a minimum this report will include the following:

- A brief synopsis of what has occurred
- An account of the information concerned in the breach
- Any initial remedial steps that have been taken to secure the breached data
- Any further recommendations that may be required
- Whether the breach needs to be reported to the Information Commissioner's Office

Where evidence suggests a breach of personal data has not occurred the records will reflect that a security incident was reported, and no breach of personal data occurred, and senior management will be informed.

4. Breach Notifications

Where the data protection officer determines a breach has occurred, the severity of the breach will need to be assessed and established. ICO guidance stipulates that the likelihood and severity of risk to people's rights and freedoms must be established.

If it is likely that the breach will have a significant impact on the rights or freedoms of individuals, then it must be reported to the data controller or the ICO. This will be determined by the data protection officer.

If it is likely that the breach will not have a significant impact on the rights or freedoms of individuals, then it may not be reported to the data controller or the ICO. It will be the decision of the data protection officer to not report the incident.

All breaches of personal data will be reported to the company director who may take any action forward as an internal matter where appropriate.

5. Reporting Breaches where RCNS Ltd is the Data Controller

Where it has been established that RCNS Ltd is the data controller and the risk to people's rights and freedoms has been assessed as likely and high, the data protection officer will report the breach to the ICO directly.

Where possible the report will be made within 24 hours. If not technically feasible to report the breach within this timescale it will be made as soon as possible thereafter. Only significant technical reasons will be acceptable in delaying the report.

6. Reporting Breaches where RCNS Ltd is the Data Processor

Where it has been established that RCNS Ltd is the data processor and the risk to people's rights and freedoms has been assessed as likely and high, the data protection officer will report the breach to the data controller directly.

Where possible the report will be made within 12 hours to enable the data controller to report the breach to the ICO within the 72-hour timescale. If it is not technically feasible to report the breach within this timescale, it will be made as soon as possible thereafter. Only significant technical reasons will be acceptable in delaying the report.

7. ICO Investigation and Responses

The data protection officer will liaise with the ICO should the ICO choose to investigate a reported breach. The data protection office will compile all responses to the ICO and will liaise with the company director prior to sending any response to the ICO.

The data protection officer will ensure any recommendations made by the ICO are complied with, within the desired timescales.

At any time, the directors of RCNS Ltd may be called upon by the ICO to answer a case and provide evidence.

8. The right to be informed

RCNS Ltd recognises the right to be informed and will provide each data subject access to a copy of this privacy policy before commencement of the processing of personal information.

9. Subject Access Requests

RCNS Ltd recognises the right to access any personal and sensitive information processed from the data subject, or in the case of a client, any lawfully appointed representative, in the form of a subject access request. RCNS Ltd will provide any information requested under the right to access, free of charge.

All subject access requests must be made in writing and sent to the data protection officer directly. Additional steps may be required to ensure the requestor is legally entitled to the information being requested. All requests will be completed within 28 working days.

10. Rectification

RCNS Ltd recognises the right to rectify any personal and sensitive information processed about a data subject, or in the case of a client, any lawfully appointed representative. RCNS Ltd will make any required rectification requested under the right to rectification, free of charge.

All rectification requests must be made in writing and sent to the data protection officer directly. Additional steps may be required to ensure the requestor is legally entitled to make the request. All requests will be completed within 28 working days.

11. Erasure of Information

RCNS Ltd recognises the right to erasure and will consider all requests on a case-by-case basis. Requests may only be denied where significant legal or technical reasoning prevents the destruction of records. Where records are not deleted, the right to restrict processing will automatically be considered as an alternative.

All erasure requests must be made in writing and sent to the data protection officer directly. Additional steps may be required to ensure the requestor is legally entitled to make the request. All requests will be responded to within 28 working days.

Where the request is denied, a full explanation of the request will be provided and the right to restrict processing will be enacted.

12. Restriction of Processing

RCNS Ltd recognises the right to restrict the processing of personal and sensitive information and will consider all requests on a case-by-case basis, requests may only be denied where significant legal or technical reasoning prevents the destruction of records.

All restriction requests must be made in writing and sent to the data protection officer directly. Additional steps may be required to ensure the requestor is legally entitled to make the request. All requests will be responded to within 28 working days.

13. Data Portability

RCNS Ltd recognises the right to portability and will cooperate with the relevant data controller as required. Where possible RCNS Ltd will aim to have the request competed within 28 days.

14. Accountability and Governance

RCNS Ltd has implemented the following data protection policies:

- RCNS Ltd Privacy Policy
- RCNS Ltd Customer Data Processing & Sharing Agreement
- RCNS Ltd Information Sharing Agreement
- RCNS Ltd Breach and GDPR Rights Policy

All policies relating to the processing of personal and sensitive information will be reviewed on an annual basis.

RCNS Ltd has appointed a specific individual to perform the functions of a data protection officer.

Any concerns regarding data protection, privacy or information governance can be reported in confidence to contact@rowleycns.co.uk.

Any requests in relation to the rights of the data subject detailed in this document must be made in writing by post or by emailing contact@rowleycns.co.uk. All requests will be handled by the data protection officer.

15. Policy Review

15.1 This policy is reviewed annually an updated accordingly.