RCNS Breach and GDPR Rights Policy

Introduction and description. This policy sets out how Rowley Clinical Neuropsychology Services Limited (RCNS Ltd) reports and handles personal data breaches and subject access requests, and how it upholds individual rights under the UK GDPR and the Data Protection Act 2018.

1. Definitions

For the purpose of this policy the following definitions apply:

- **RCNS Ltd** means Rowley Clinical Neuropsychology Services Limited, registered in England and Wales with Companies House under company number 13832672.
- **Company head office** means RCNS Ltd, International House, 14 King Street, Leeds, England, LS1 2HL.
- **Associates** means qualified clinical psychologists who provide psychology services on a case and who are legally separate trading entities (self-employed sole traders or limited companies) appointed by RCNS Ltd.
- **UK GDPR** means the retained version of the General Data Protection Regulation (EU) 2016/679 as it forms part of UK law.
- **DPA 2018** means the Data Protection Act 2018, as amended.
- **Data subject** means the individual whom particular personal data is about.
- **Data controller** means the person or organisation that, alone or jointly with others, decides the purposes and means of processing personal data.
- **Data processor** means a person or organisation that processes personal data on behalf of a data controller.
- **Processing** means any operation carried out on information or data, including obtaining, recording, holding, sharing and deleting it.
- **ICO** means the Information Commissioner's Office, the UK regulator for data protection and information rights.
- **Responsible director** means the director of RCNS Ltd who leads on data protection and carries out the investigations, reports and request handling set out in this policy.
- **Individual rights** means the rights individuals have under the UK GDPR, set out in sections 8 to 15.

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:

- Any personal data is lost, destroyed, corrupted or disclosed.
- Someone accesses the data or passes it on without proper authorisation.

- 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 are given below. 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 special category data shared with RCNS Ltd must be investigated to determine whether a personal data breach has occurred.

3. Investigation

Where an incident occurs that may constitute a personal data breach, it must be reported immediately to the responsible director, who will in all instances fully investigate it.

All potential incidents reported to the responsible director are recorded permanently and may be referred to in future investigations.

The responsible director will be given full access to the facts and all information relating to the incident. During the investigation they may collect the following:

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

The steps taken are not limited to the points above. All necessary steps will be taken to give a comprehensive overview of the incident.

Where evidence suggests that a personal data breach has occurred, the records will say so and a formal report will be produced. As a minimum the report will include:

- A brief synopsis of what has occurred
- An account of the information concerned in the breach
- Any initial remedial steps taken to secure the data
- Any further recommendations that may be required
- Whether the breach needs to be reported to the ICO, the data controller or the individuals affected

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

4. Breach notifications

Where the responsible director determines that a breach has occurred, they will assess the likelihood and severity of the risk to people's rights and freedoms, following ICO guidance.

- **Where RCNS Ltd is the data controller:** the breach must be reported to the ICO unless it is unlikely to result in a risk to individuals. If the breach is likely to result in a high risk to individuals, they must also be told without undue delay.
- **Where RCNS Ltd is the data processor:** every breach must be reported to the relevant data controller without undue delay, whatever the level of risk.

Every breach is recorded, whether or not it is reported, including the facts, its effects and the action taken. A record of every personal data breach is retained indefinitely.

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

5. Reporting breaches where RCNS Ltd is the data controller

Where RCNS Ltd is the data controller and the breach must be reported, the responsible director will report it to the ICO without undue delay and no later than 72 hours after becoming aware of it. If full details are not yet available, an initial report will be made within this time and further information provided as it becomes known.

6. Reporting breaches where RCNS Ltd is the data processor

Where RCNS Ltd is the data processor, the responsible director will report the breach to the data controller directly, without undue delay and where possible within 12 hours, so that the data controller can report it to the ICO within the 72-hour timescale. Only significant technical reasons will be acceptable in delaying the report.

7. ICO investigation and responses

The responsible director will liaise with the ICO should the ICO choose to investigate a reported breach. They will compile all responses to the ICO and will liaise with the other directors before sending any response.

The responsible director will ensure any recommendations made by the ICO are complied with within the required 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 give each data subject access to a copy of the RCNS Ltd Privacy Policy before we start processing their personal information.

9. Subject access requests

RCNS Ltd recognises the right of access to any personal and special category data it processes about a data subject or, in the case of a client, about the client by any lawfully appointed representative. RCNS Ltd will provide the information requested free of charge.

Requests can be made verbally or in writing, but to make sure they are handled promptly we ask that they are sent in writing to the responsible director (see section 16). Additional steps may be required to confirm the requestor is legally entitled to the information. All requests will be completed within one month of receipt. For complex or numerous requests this may be extended by up to two further months, and the requestor will be told if so.

10. Rectification

RCNS Ltd recognises the right to have inaccurate or incomplete personal and special category data corrected, whether requested by the data subject or, in the case of a client, by any lawfully appointed representative. RCNS Ltd will make any required rectification free of charge.

Requests should be sent in writing to the responsible director. Additional steps may be required to confirm the requestor is legally entitled to make the request. All requests will be completed within one month of receipt, extendable as in section 9.

11. Erasure of information

RCNS Ltd recognises the right to erasure and will consider all requests case by case. A request may be refused only where significant legal or technical reasons prevent records being destroyed, for example the retention periods in the RCNS Ltd Privacy Policy. Where records are not deleted, the right to restrict processing will automatically be considered as an alternative.

Requests should be sent in writing to the responsible director. Additional steps may be required to confirm the requestor is legally entitled to make the request. All requests will be responded to within one month of receipt, extendable as in section 9.

Where a request is refused, a full explanation will be provided and the right to restrict processing will be put in place.

12. Restriction of processing

RCNS Ltd recognises the right to restrict the processing of personal and special category data and will consider all requests case by case. A request may be refused only where significant legal or technical reasons prevent it.

Requests should be sent in writing to the responsible director. Additional steps may be required to confirm the requestor is legally entitled to make the request. All requests will be responded to within one month of receipt, extendable as in section 9.

13. Data portability

RCNS Ltd recognises the right to data portability and will cooperate with the relevant data controller as required. Requests will be completed within one month of receipt where possible.

14. Objection and automated decision-making

RCNS Ltd recognises the right to object to processing. The right does not apply where processing is necessary for a contract or to meet a legal obligation, which are the bases RCNS Ltd relies on.

RCNS Ltd does not carry out profiling and does not rely on automated decision-making.

15. Complaints

If you are unhappy with how RCNS Ltd has handled your information, please contact us first (see section 16). You can also complain to the Information Commissioner's Office at ico.org.uk or on 0303 123 1113.

16. Accountability and governance

RCNS Ltd has implemented the following data protection policies:

- RCNS Ltd Privacy Policy
- RCNS Ltd Information Sharing Agreement
- RCNS Ltd Breach and GDPR Rights Policy

All policies relating to the processing of personal and special category data are reviewed annually.

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

Any request relating to the rights of the data subject in this document can be made in writing by post to the company head office or by email to contact@rcns.co.uk. All requests will be handled by the responsible director.

17. Policy review

This policy is reviewed annually and updated as needed.