

# RNC Policy & Procedure: Data Protection

|  |  |
| --- | --- |
| Responsibility: | Technical Support Manager |
| Approved by SMT: | June 2023 |
| Date of next review: | June 2024 |
| EIA Completed: | October 2017 |
| EIA Reviewed: | March 2022 |
| Other relevant Policies and reference documents:Data Retention and Disposal PolicyData Backup PolicyCCTV PolicyAcceptable Use Policy Computing and IT Systems and Resources PolicySecure Archiving PolicyDisciplinary PolicyGrievance Policy |
| Version | Date | Amendments | Author  |
| 1.0 | 30/05/18September 2018 | GDPR Updates. FormattingSMT approval | POK/AP |
| 1.1 | July 2019 | Changes to Designated Data Controller | POK/AP |
| 1.2 | November 2020 | Policy reviewed, amended job titles, Data Protection Incident log, GDPR, referenced Smartlog training | AP |
| 1.3 | January 2022 | General updating and formatting. GDPR(EU) amended to UK GDPR. Section 3 updated legislation. Added new Section 4 Privacy Notices. Section 6 updated included DPIA. Section 9 updated. Added new Section 14 International Transfers | AP |
| 1.4 | June 2023 | Minor updating. Removed tech old extension numberSection 13 removed (examination and accreditation results) | AP |

**Commitment Statement**

RNC is committed to the fundamental values of equality, diversity and inclusion, which creates a supportive environment for all members of our community to live, work and study. Our commitment to equality and diversity means that this policy has been screened in relation to the use of plain English, the promotion of the positive duty in relation to race, gender and disability and to eliminate discrimination to other equality groups related to age, sexual orientation, gender identity, marital or civil partnership status, pregnancy or maternity and religion or belief. We believe that safeguarding has paramount importance and RNC recognises its responsibility and duties within the Government Prevent Strategy to be aware of and where appropriate act to ensure the safety of all students from radicalisation and extremism.

This document is available in alternative formats on request. If you think RNC can improve the fairness of this policy please contact the author who has responsibility for the review and update.

## Contents

[RNC Policy & Procedure: Data Protection 1](#_Toc140481022)

[Contents 3](#_Toc140481023)

[1. Definitions 4](#_Toc140481024)

[2. The Data Controller and the Designated Data Controller/s 4](#_Toc140481025)

[3. Introduction 4](#_Toc140481026)

[4. Privacy Notices 5](#_Toc140481027)

[5. Data Subjects’ Rights 5](#_Toc140481028)

[6. Responsibilities of staff 6](#_Toc140481029)

[7. Data security 7](#_Toc140481030)

[8. Student obligations 7](#_Toc140481031)

[9. Data Protection Incidents 7](#_Toc140481032)

[10. Publication of RNC Information 7](#_Toc140481033)

[11. Processing sensitive information 8](#_Toc140481034)

[12. Subject consent 8](#_Toc140481035)

[13. International Transfers 8](#_Toc140481036)

[14. Retention of Data 8](#_Toc140481037)

[15. Conclusion 8](#_Toc140481038)

**Data Protection**

## Definitions

For the purposes of this policy document, the following definitions will apply:

Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly from this data and other information, which is in the possession of, or is likely to come into the possession of, the data controller.

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on the data. It includes organising, adapting and amending the data, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data.

## The Data Controller and the Designated Data Controller/s

RNC as a body corporate is the data controller and data processor under the Data Protection Act 2018 and is registered (Z7570441) with the Information Commissioner’s Office (ICO). The Board is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters.

RNC has two Designated Data Controllers. They are the Executive Principal and the Technical Support Manager.

## Introduction

RNC needs to keep certain information about its employees, students and other individuals to allow it to, for example, monitor performance, achievements, and health and safety. It is also necessary to produce information so that staff can be recruited and paid, courses and study programmes organised, legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the organisation must comply with the Data Protection principles, which are enshrined in UK law by the Data Protection Act 2018 (DPA 2018) and the United Kingdom General Data Protection Regulation (UK GDPR) which came into force 1January 2021.

The UK GDPR sets out seven key principles which lie at the heart of the general data protection regulations:

* **Lawfulness, fairness, and transparency**

RNC processes personal data lawfully, fairly and in a transparent manner

* **Purpose limitation**

RNC collects personal data only for specified, explicit and legitimate purposes

* **Data minimisation**

RNC processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing

* **Accuracy**

RNC keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay

* **Storage limitation**

RNC keeps personal data only for the period necessary for processing

* **Integrity and confidentiality (security)**

Personal data must be kept safe from unauthorised access, accidental loss or destruction

* **Accountability**

RNC and all staff or others who process or use any personal information must ensure that they follow these principles at all times. Inorder to ensure that this happens, RNC has developed this Data Protection Policy.

It is a condition of employment that employees will abide by the policies and procedures made by the organisation. Therefore, any failures to follow the policy may result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

##  Privacy Notices

The organisation will issue privacy notices informing the people from whom we collect information about the personal data that we collect and hold relating to them, how they can expect their personal data to be used and for what purposes.

RNC will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

##  Data Subjects’ Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

* where the legal basis of our processing is Consent, to withdraw that Consent at any time
* to ask for access to the personal data that we hold (see below)
* to prevent our use of the personal data for direct marketing purposes
* to object to our processing of personal data in limited circumstances
* to ask us to erase personal data without delay:
* if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed
* if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data
* if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest
* if the data subject has objected to our processing for direct marketing purposes
* if the processing is unlawful
* to ask us to rectify inaccurate data or to complete incomplete data
* to restrict processing in specific circumstances e.g. where there is a complaint about accuracy
* to ask us for a copy of the safeguards under which personal data is transferred outside of the EEA
* the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with RNC; it is based on the data subject’s explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards
* to prevent processing that is likely to cause damage or distress to the data subject or anyone else
* to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
* to make a complaint to the ICO
* in limited circumstances, receive or ask for their personal data to be transferred to a third party (e.g. another education provider to which a student is transferring) in a structured, commonly used and machine-readable format

You must verify the identity of an individual requesting data under any of the rights listed.

Requests (including for data subject access) must be complied with, usually within one month of receipt.

##  Responsibilities of staff

All staff are responsible for:

* Checking that any information that they provide to the organisation in connection with their employment is accurate and up to date
* Informing the organisation of any changes to information, which they have provided, for example a change of address
* Checking the information that the organisation will send out from time to time, giving details of information kept and processed about staff
* Informing the organisation of any errors or changes. The organisation cannot be held responsible for any errors unless the staff member has informed the organisation of them

Staff members who process personal data about students, customers, staff, applicants, alumni or any other individual must comply with the requirements of this policy. Staff members must ensure that:

* all personal data is kept securely
* no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
* where processing is likely to result in a high risk to an individual’s data protection rights before commencing and processing a Data Privacy Impact Assessment (DPIA) must be undertaken
* personal data is kept in accordance with the RNC Data Retention Policy
* any queries regarding data protection, including subject access requests and complaints, are promptly directed to the designated Data Controllers
* all data protection breaches are reported in accordance with section 9 of this policy
* where there is uncertainty around a data protection matter advice is sought from the Technical Support Manager or designated Data Controllers

Where members of staff are responsible for supervising students doing work, which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection principles.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the designated Data Controllers.

A data protection training module is available on the Smartlog training portal, which all staff who have access to personal identifiable data will be expected to complete.

## Data security

Personal information should be:

* kept in a locked filing cabinet; or
* in a locked drawer; or
* if it is computerised, access should be restricted; or
* kept only on a medium which is itself kept securely

## Student obligations

Students must familiarise themselves with the Privacy Notice on the RNC website and ensure that all personal data provided to the organisation is accurate and up to date. They must ensure that they notify the Registry Department or appropriate persons of any changes of address etc.

Students who use the organisation’s computer facilities may, from time to time, process personal data. If they do, they must notify the data controller. Any student who requires further clarification about this should contact the data controller.

## Data Protection Incidents

In the event of personal data being made available to unauthorised individuals, for whatever reason, staff are required to **immediately** fill in a Data Protection Incident Form located on the Data Protection SharePoint site. Please contact Technical Support helpdesk or email tech@rnc.ac.uk.

When an incident is logged, a chain of events is set in motion and the Technical Support Manager will investigate and perform an in-depth analysis to check if any data protection or internal security rules have been breached. Where applicable the Technical Support Manager will immediately put in place a recovery plan, including damage limitation and notify the Executive Principal.

The Executive Principal is ultimately responsible for ensuring that all necessary individuals and organisations are informed of the incident. These are decided on a case-by-case basis but the following should be considered:

* any individuals concerned
* the Information Commissioner's Office (ICO)
* relevant regulatory bodies
* other third parties, such as law enforcement and financial bodies
* the media

A notifiable data breach must be reported to the ICO without undue delay and, where possible within 72 hours of becoming aware of it.

After the incident has been dealt with, the Technical Support Manager will conduct a review of the response and present an action plan to SMT.

## Publication of RNC Information

Information that is already in the public domain is exempt from the DPA 2018. It is the policy of the organisation to make as much information public as possible.

## Processing sensitive information

Sometimes it is necessary to process information about a person's health, criminal convictions, race, gender and family details. This may be to ensure that the organisation is a safe place for everyone, or to operate other organisation policies, such as the Equality, Diversity and Inclusion Policy.

In some cases, if the data is sensitive, express consent must be obtained. Agreement to the organisation processing some specified classes of personal data is a condition of acceptance of a student onto any course or study programme, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The organisation has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and students or trainees for the courses offered. The organisation also has a duty of care to all staff and students and must therefore make sure that employees and those who use the facilities of the organisation do not pose a threat or danger to other users.

The organisation may also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The organisation will only use this information in the protection of the health and safety of the individual.

## Subject consent

Sometimes the organisation can only process personal data with the consent of the individual.

In the absence of consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to RNC (e.g. students’ parents, members of the public, private property owners).

## International Transfers

RNC may transfer personal data outside the European Economic Area (EEA) to other countries on the basis that such countries are designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards or where we obtain the relevant data subjects’ explicit consent to such transfers, for example, a student application from outside of the EEA.

## Retention of Data

The organisation will keep some forms of information longer than others.

A full list of information with retention times is contained within the Data Retention Policy document.

## Conclusion

Compliance with the Data Protection Act 2018 and the United Kingdom General Data Protection Regulation is the responsibility of all stakeholders of the RNC. Any deliberate breach of the data protection policy may lead to disciplinary action, or access to the organisation facilities being withdrawn, or a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated Data Controller.