Document Title	Data Protection Policy
Type of document	Corporate
Brief summary of contents	• Clear guidance when dealing with personal data covered under Data Protection legislation • Responsibilities of individuals • Data Subject Access requests • Rights of the data subjects • Responsible parties • Privacy notices
SLT member responsible for policy	Executive Director of Strategic Planning & Corporate Services
Date written	4th February 2016
Date last revised	23rd January 2023
This document replaces	Not applicable
Approval route/consultation	Department Head, SLT Member
Head of Department (HOD) responsible for policy	Kelly Condon
Author of policy	Department Head
Contact details	DPO@rnngroup.ac.uk
Publication location	Public and portals
Date of final approval	4th February 2016
Date policy becomes live	4th February 2016
Review period	Annual
Links to external standards	Data Protection Legislation
Related documents	• Staff AUP • Mobile Phone Policy • Privacy Policy
Keywords	Privacy, data, data protection, data controller, lawful, accurate, personal, subject access, subject consent, data retention, rights
Training needs	Data Protection

This document is only valid on the day of printing

Data Protection Policy

Version 2.3

23rd January 2023

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
4th February 2016	1.0	Birth of policy	Ian Headley
27th October 2016	1.1	Change in form for Subject Access Request	Ian Headley
21st March 2017	1.2	Annual review Change in SLT member Change in contact details to RNN Group Job title changes Amendment to designated RNN Group data controllers Inclusion of Data Privacy Notice (Section 15)	Ian Headley
9th May 2018	2.0	GDPR review and updated to new legislation	Ian Headley
31st May 2019	2.1	Annual review No amendments	Ian Headley
6th December 2019	2.2	Annual review Minor changes to contact details and job titles	Kelly Condon
23rd January 2023	2.3	Annual review Addition of Accountability principle Minor changes to grammar and format Addition of Google to cloud providers. Amendment to department name.	Kelly Condon

Table of Contents

Appendices

Policy Outline

Introduction

RNN Group is committed to preserving the privacy of its learners and employees and to complying with the Data Protection UK laws. To achieve this commitment, information about our learners, employees and other clients and contacts must be collected, used fairly, stored safely and not unlawfully disclosed to any other individual or organisation.

It is the Group's policy to make as much information public as possible and in particular, the following information will be made available.

- Names of our Governors
- Photographs of key staff (i.e. members of the Executive and other managers)
- Data retention periods
- Third parties to whom we share or allow access to the data we collect
- Privacy notices

Principles

The Group, its staff and others who process or use any personal information will ensure that they follow the data privacy principles set out in the UK Data Protection legislation. These principles are:

a) Lawfulness, fairness and transparency
b) Purpose limitation
c) Data minimisation
d) Accuracy
e) Storage limitation
f) Integrity and confidentiality (security)
g) Accountability

The Group will not release staff or learner data to third parties except to relevant statutory bodies or where the relevant RNN Group Third Party Agreement is in place.

In all other circumstances, the Group will have informed the data subjects as to what happens to their data at the initial collection point and shall, where deemed necessary, obtain the consent of the individuals concerned before releasing personal data.

Responsibilities of Staff

Corporation Board

The Corporation Board are responsible for the oversight and implementation of this policy.

The Chief Executive and Senior Managers

It will be the responsibility of the CEO & Principal and members of the Senior Leadership Team (SLT) to ensure compliance with the policy and for communicating the policy to all staff.

Data Protection Officer

The Data Protection Officer for the Group has operational responsibility for the implementation of this policy throughout the Group and is the initial point of contact for any Data Protection related enquiries.

The designated Data Guardians (as detailed in Section 5) have specific responsibilities for the areas they are responsible for.

Managers

All Managers are responsible for ensuring that staff are aware of, and abide by, this policy and that their relative staff members have participated in the Group's Data Protection training.

All Staff

All staff are responsible for ensuring that any personal data which they hold is kept securely, transported safely (where approved by the Information Governance and Assurance (IGA) team) and that personal information is not disclosed in any way and to any unauthorised third party. Personal data referred to can be either paper or electronic based, in any format.

It is the duty of all Group staff to report data breaches and near miss events relating to the processing of personal data, to the IGA team as soon as they become 'aware' of a breach.

Awareness is defined as when a member of staff has a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised.

Sanctions can be applicable to the Group should we fail in our obligations under the UK Data Protection laws to report a data breach to the ICO, these could potentially be damaging to our reputation.

The Data Protection Act 2018 explains that a personal data breach can be categorised as:

"Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data

"Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data

"Integrity breach" - where there is an unauthorised or accidental alteration of personal data

This reporting can be done directly to the IGA team, by phone, email or via the online reporting tool on the RNN Group Information Governance and Assurance website. Learners or members of the general public can also make reports should they wish to express concern, by using the same mechanisms.

All staff are required to participate annually in the RNN Group Data Protection mandatory training.

All Learners, Staff and Other Parties

Learners, staff and other related parties are responsible for ensuring that all personal data provided to the Group is accurate and up to date.

Compliance

Failure to comply with the data protection policy and procedure may result in disciplinary action.

Review

This policy and related procedures will be reviewed and issued on at least an annual basis.

Data Privacy and Protection

1. Introduction

1.1 The RNN Group (hereinafter referred to as the 'Group') needs to keep certain information about its employees, learners and other users to allow the Group to deal with numerous aspects of the business, including monitoring recruitment, attendance, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

1.2 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 Group must comply with the Data Protection Principles, which are set out in the UK Data Protection legislation.

1.3 These principles are:

h) Lawfulness, fairness and transparency
i) Purpose limitation
j) Data minimisation
k) Accuracy
l) Storage limitation
m) Integrity and confidentiality (security)
n) Accountability

1.4 The Group and all staff or others who process or use any personal information collected by the Group must ensure that they follow these principles at all times. In order to ensure that this happens, the Group has developed the Data Protection Policy.

1.5 The Group will keep a register of staff authorised to access and process personal data on its systems with the appropriate security restrictions and these members of staff will be asked to agree to a confidentiality statement on network login.

2. Responsibilities of Staff

Information About Individual Staff Members

2.1 All staff are responsible for:

- Checking that any information provided to the Group in connection with their employment is accurate and up-to-date.
- Informing the Group of any changes to information which they have provided, e.g. change of address.
- Informing the Group of any errors. The Group cannot be held responsible for any errors unless there is clear evidence that the staff member submitted an appropriate request for change.

Information About Other People

2.2 All staff must comply with the following guidelines:

a) All staff will process data about individuals on a regular basis, for example, when marking registers, writing reports or references, as part of the employment process, or as part of a pastoral or academic supervisory role.

b) The Group will ensure through internal procedures, that all individuals are informed of the lawful basis for the processing of their data, are notified of the categories of processing and the purpose for the data collection itself, as required by the UK Data Protection legislation.

c) The information that staff deal with on a day-to-day basis will predominantly be personal information and will cover categories such as:

- General personal details such as name and address
- Details about class attendance, course work marks and grades and associated comments
- Notes of personal supervision, including matters about behaviour and discipline

Information about an individual's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning health
- data concerning sex life or sexual orientation

are all classed as special categories of data and can only be collected and processed with the explicit consent of the individual and within the same conditions as personal data collection, for example having a lawful basis for processing, purpose for the collection etc.

d) All staff have a duty to make sure that they comply with the data protection principles, which are set out in the Group's Data Protection Policy. In particular, staff must ensure that records are:

- Accurate
- Up-to-date
- Limited to what was specified originally to the data subject
- Kept and disposed of safely, and in accordance with the Group's policies

e) The Group will designate staff in the relevant area as 'authorised staff' through appropriate security mechanisms. These staff are the only staff authorised to access data that is:

- Not standard data or

- Special categories data

f) The only exception to this will be if a non-authorised member is satisfied and can demonstrate that the processing of the data is necessary for the vital interests of the data subject themselves, as:

   - In the best interests of the individual or staff member, or a third person, or the Group AND
   - The individual has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances
   - This should only happen in very limited circumstances, e.g. an individual is injured and unconscious and in need of medical attention, or a member of staff tells the Hospital that the individual is pregnant.

g) Authorised staff will be responsible for ensuring that all personal data is kept securely. In particular staff must ensure that:

   - Personal data is put away in lockable storage
   - Personal data is not left on unattended desks or tables
   - Unattended IT equipment should not be accessible to other users
   - IT equipment used off-site must be encrypted (including tablets, mobile phones etc.), or password protected where encryption is not possible
   - Data on portable media e.g. a memory stick, or any mobile device storage that contains personal data or email attachments used off-site, must be encrypted or password protected should encryption not be possible
   - Paper records containing personal data must be shredded or placed into confidential waste consoles where appropriate (and in line with the relevant retention policy)
   - Personal data records are **NOT** stored on any personal cloud storage provider or personal mobile devices (the RNN Group provided Google and Office 365 environment are the only approved cloud providers for the storage of personal information)

h) Staff must not disclose personal data to any individual, unless for normal academic or pastoral purposes, without authorisation or in line with the Group's Data Subject Access Request (DSAR) policy.

i) Staff shall not disclose personal data to any other non-authorised staff member except with the authorisation of a data guardian or the DPO.

j) Before processing any personal data, all staff should consider the following:

   - Does the information really need to be recorded?
   - Has a Data Privacy Impact Assessment (DPIA) been performed on the data collection set?
   - Is the information classified as being 'special category' data?
   - If it is special category, has the data subject provided express consent via a positive affirmative action, along with the lawful basis?
   - Has the individual been told that this type of data will be processed?

- Is the staff member authorised to collect/store/process the data?
- If yes, has it been confirmed with the data subject that the data is accurate?
- Is it certain that the data is secure?
- If the data subject's consent to process has not been obtained/provided, can it be confirmed satisfactorily that it is in the vital interests of the individual or the safety of others to collect, process and retain the data?

3. Rights to Access Information

3.1 Learners, staff, individuals and other users of the Group's services have the right to access any personal data that is being kept about them either electronic or paper based. Any person who wishes to exercise this right must complete the Group's Data Subject Access Request (DSAR) form and send it to the IGA team at the email address given on the form (Appendix 2).

3.2 This information will, in most cases, be supplied without charge. The Group's DPO will decide on a case by case basis if any charge for large volumes of data requests is applicable.

3.3 The Group aims to comply with requests for personal data as quickly as possible, will ensure that it is provided without undue delay and within one calendar month (in line with legislation) unless there is valid reason for delay as determined by the Group's DPO on a case by case basis. In such cases, the reason for delay will be explained in writing to the data subject making the request.

4. Subject Consent

4.1 In many cases, the Group can only collect and process special categories of data with the positive affirmative action in consent by the data subject themselves.

4.2 Agreement to the Group processing certain specified classes of personal data is a condition of the acceptance of an individual onto any course, and a condition of employment for staff. This includes details about previous criminal offence data.

4.3 Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 14 and 18. The Group has a duty under the Children Act and other legislation to ensure that staff are suitable for any job offered.

4.4 The Group also has a duty of care to all staff and learners and must therefore make sure that employees and those who use the Group's facilities do not pose a threat or danger to other users.

4.5 The Group will 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 Group will only use the information in the protection of the health and safety of the individual and may not need consent to process this type of information, in the event of a medical emergency, for example.

4.6 All prospective staff and learners will be asked to sign either an appropriate Human Resources form or another individual document regarding special categories of data

when an offer of employment or a course place is made. A refusal to sign such documents may result in the offer being withdrawn.

5. The Data Controller and the Designated Data Guardians

5.1 The Group as a corporate body is the data controller under UK Data Protection legislation, and the Board is therefore ultimately responsible for compliance. However, the designated Data Guardians will deal with day-to-day matters.

5.2 The nominated Data Protection Officer is the primary contact for any data related enquiries or events. In the event of the DPO not being unavailable, the nominated deputy is the Data Protection Advisor (DPA) in the first instance.

5.3 The Group's designated data guardians are the Director of Strategic Planning and Corporate Services who is responsible for all corporate data and for storage, retrieval and destruction of the data relating to IT. The Executive Director of Human Resources, Organisational Development and Marketing who is responsible for all data relating to staff. The Executive Director of Finance who is responsible for data relating to Estates and Finance including Group subsidiaries, and the Head of MIS for all data relating to learners.

6. Transfer of Information to Data Processors and Sub-Contractors

6.1 Any third party or contractor who has access to the Group's obtained personal data and/or is acting as data processor should be fully aware of their obligations to comply with the Data Protection legislation, be registered with the ICO and be contracted to act accordingly using the Group's Third Party Agreements. This includes any contractor who is accessing areas where obtained personal data is stored or can be viewed/accessed.

No data will be transferred or made available to any party unless the Third Party Agreement and/or relative contract is completed and registered with the Data Protection Officer in advance.

6.2 Personal data will not be transferred to any country outside the European Economic Area (EEA) unless there is adequate protection in place through local data protection laws, organisational policies or contractual agreements.

7. Retention of Data

7.1 Data will be retained subject to the explicit data retention periods as specified in the individual policies or procedures and specific to the data being collected. These periods are identified through the DPIA programme throughout the Group.

7.2 Further details of all the data retention periods whether Group dictated or legislatively required, are available on the Group website.

8. Notification of Change to the Processing of Personal Data

8.1 The existing Data Protection registration for the Group can be found at: https://ico.org.uk/esdwebpages/search

8.2 Any changes will be reflected on this site and notified to appropriate staff.

9. Conclusion

9.1 Compliance with the relevant Data Protection legislation is the responsibility of all members of the Group and appropriate mandatory training ir provided to all Staff members.

9.2 Any breach of the data protection policy may lead to disciplinary action being taken, access to Group systems being withdrawn, or even a criminal prosecution.

9.3 Any questions or concerns about the interpretation of this policy should be referred to your line manager or the IGA team.

10. Data Privacy Notice

10.1 Under the UK Data Protection legislation and the Information Commissioner's Office Privacy Notices Code of Practice, privacy notices should be present at all collection points where personal data is being collected from a data subject, especially if the data is being collected for a new purpose.

10.2 The Group employs a layered approach to this notification, the relevant data collection set notice will be specific to the data being collected and its lawful basis determined through the DPIA process. An A4 notice should be at any collection point (content detail below) and the full privacy policy of the Group is available on all of its websites.

10.3 A4 privacy notices are available from the IGA team at IG@rnngroup.ac.uk and contain the following information:

- What the Group needs
- Why the Group needs it
- What the Group will do with it
- How long the Group keep it
- What the Group would also like to do with it
- What are the individual's rights

11. Data Subject Rights

11.1 It is the Group's responsibility to uphold all of the rights of the data subject as described in UK Data Protection legislation. These rights are specifically:

- Transparent communication
- Information to be provided to the data subject e.g. controller details, DPO, third parties with access etc.
- Information to be provided where personal data was not obtained from the data subject
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Notification of rectification or erasure

- Right to data portability
- Right to object to processing
- Right to object to automated profiling decision making

11.2 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK Data Protection regulations.

11.3 The Group must provide individuals with information including our purposes for processing their personal data, retention periods for that personal data, and to whom it will be shared with. This is called 'privacy information'.

11.4 Privacy information must be provided to individuals at the time that personal data is collected from them.

11.5 If the Group obtains personal data from other sources, then these individuals must be provided with privacy information within a reasonable period of obtaining the data and no later than one month. There are a few circumstances when the Group does not need to provide people with privacy information, such as if it would involve a disproportionate effort to provide it to them.

11.6 The information the Group provides to people must be concise, transparent, intelligible, easily accessible, and must use clear and plain language.

11.7 The Group regularly reviews, and where necessary, updates the privacy information. Any new uses of an individual's personal data must be brought to their attention before processing begins.

Appendix 1 – Collection point privacy notice

Your privacy is important to us

When you choose the RNN Group, you trust us with your information.
We take that responsibility very seriously.

What we need

The RNN Group is what is known as 'the controller' of the personal data you provide to us. We collect not only basic personal data about you, things like your name, address, email etc. but may sometimes need to collect some special categories of information such as ethnic origin, data concerning health etc.
The RNN Group has a Data Protection Officer, the DPO can be contacted directly by emailing dpo@rnngroup.ac.uk.

Why we need it

We need to know your basic personal data in order for us to provide you with details regarding your interaction with the RNN Group. We may also have legal obligations under UK legislation to collect data from you and will always process data where your vital interests are concerned or if it is in the public interest to do so. We will not collect any personal data from you that we do not need in order to provide and oversee any services to yourself.

What we do with it

All of the personal data we collect is processed by our staff in the UK however for the purposes of IT hosting and maintenance, this information may be located on servers within the European Union and occasionally, trusted parties outside the EU may have access to certain parts of the data we collect. No third parties have access to your personal data unless UK legislation allows them to do so or an official processing agreement is in place with the RNN Group. A full copy of our privacy policy is available on our website www.rnngroup.ac.uk.

How long we keep it

There are various retention periods set for the Group, some relating to UK legislation, the data we collected will be destroyed or anonymised when these dates are reached. Your information that we use for marketing purposes will be kept until you notify us that you no longer wish to receive this type of information. More information on our data retention schedule can be found online at www.rnngroup.co.uk.

What we would also like to do with it

The RNN Group may use some of the data that we have collected, such as your name and email address, to inform you of our future offers and similar products. This information is not shared with, or sold to, third parties and you can unsubscribe at any time via the unsubscribe option, phone or on our website. Sometimes this data will be stored outside of the EU.

What are your rights?

We will not always need consent to use your personal information, for example, if we need it to meet regulatory requirements. Sometimes however, your express consent will be required, for example if we are collecting data regarding your health, this will be explained when we collect the data.
If at any point you believe the information we process on you is incorrect, you can request to see this information and even have it corrected or deleted, simply email sar@rnngroup.ac.uk outlining your specific requirements.
If you wish to raise a complaint about how we have handled your personal data, please email complaints@rnngroup.co.uk with full details of your issue.
If you are not satisfied with our response or believe we are processing your personal data not in accordance with the law, you can complain to the Information Commissioner's Office (ICO) www.ico.org.uk.

Appendix 2 – Data Subject Access Request form

Data Subject Access Request Form

Staff, learners (and other users of the RNN Group) have the right to access personal data relating to themselves that is held by the Group in electronic and/or manual records that form part of a 'relevant filing system'.

Any individual who wishes to exercise this right should apply using this Data Subject Access Request (DSAR) form in the first instance.

The RNN Group needs to be assured of an applicant's identity prior to any information being released. To protect the data that has been trusted to us, due diligence on this request will be performed before any acknowledgement or release. Data requested will be supplied, where possible, in PDF format, encrypted and emailed or posted to our secure portal. The applicant will receive a link to the portal where they will be asked for a password, which will be sent in a separate email.

The RNN Group may hold personal records in different parts of its organisation, to assist us to supply the information you require, please provide the following information:

Details
Surname: Former Surname (if applicable): Forename(s): Date of birth: Address: Postcode: Telephone number: Email address:

Learner
Are you a present or past learner of the RNN Group?: Give details of your course of study and dates:

Staff
Are you a present or past member of staff?: Department/Area of the RNN Group: For past staff, please give dates and as much detail of employment as possible:

Other (neither staff nor learner)
If you are neither staff nor learner, please detail your connection with the RNN Group or detail your relationship to the person you are requesting data for. Written consent from the individual will be required prior to data being released, this authority MUST be enclosed with the DSAR:

Information required
The RNN Group may hold your personal records in different parts of its organisation. Please specify the information you require and be as specific as possible to help us process and expedite your request (continue on separate sheet if needed): Examples of data kept by the RNN Group • Academic marks or course work details • Personnel records • Health and medical matters • Additional Learning Support (ALS) records • Personal details including name, address, date of birth etc. Information required (use the above example/s or provide further details below):

Your signature:	Date:

On completion, this form and any supporting information should be sent to:

Email: sar@rnngroup.ac.uk

Post:
For the attention of the Information Governance and Assurance Team
RNN Group
Eastwood Lane
Rotherham
S65 1EG

Privacy and Data Protection Accountability Statement

Responsible Body: RNN Group
Purpose: To validate the details you have provided, to enable the appropriate data searches to take place and to facilitate additional contact, should this be necessary
Lawful Basis: Contract and legal obligation
Recipients: Data will not be transferred to third parties except where a legal obligation exists or that it is required for the Group to perform its duties
Rights: Access, rectification and objection
Additional Information: More information in regards to the RNN Group's accountability and transparency framework can be found at www.rnngroup.ac.uk/IG
The RNN Group may use your name and email address to inform you of our future offers and similar products or services. This information is not shared with third parties and you can unsubscribe at any time.