Document Title	Data Subject Access Request (DSAR) Policy & Procedure
Type of document	Corporate
Brief summary of contents	• Explains the rights of individuals under current Data Protection legislation • Gives definitions of personal and sensitive data • Definition of a Data Subject Access Request (DSAR) • Responsibilities of individuals • Procedure for the supply of DSAR's • Procedural flowcharts • DSAR Forms
SLT member responsible for policy	Executive Director of Strategic Planning & Corporate Service
Date written	14th September 2016
Date last revised	17th January 2023
This document replaces	Rotherham DP SAR Any other internal data access request procedures
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	13th October 2016
Date policy becomes live	13th October 2016
Review period	Annual
Links to external standards	Data Protection Act 2018 General Data Protection Regulations (GDPR)
Related documents	• RNN Group Data Protection Policy • Privacy Policy • Staff Acceptable Use Policy (AUP) • Learner Acceptable Use Policy (AUP) • Mobile Phone Policy • Reference/Attendance Letter Provision Procedure • CCTV Policy • Archiving Policy • Data Retention Policy • Privacy Policy • Data Breach Procedure
Keywords	Data, Data Protection, GDPR, Privacy, Data Controller, Lawful, Accurate, Personal, Subject Access, SAR, DSAR, Subject Consent, Data retention
Training needs	Data Protection

Data Subject Access Request (DSAR) Policy & Procedure

Version 2.3

17th January 2023

Version Control Table

Date	Version No	Summary of Changes	Changes Made By
13th September 2016	1.0	Birth of policy	Ian Headley
13th October 2016	1.1	Minor amendments including staff references and flowchart for Student Services supplied by AAdams, DWest, CMuffett and KCondon	Ian Headley
7th December 2017	1.2	Change of SLT lead, references to GDPR included, responsibilities update with latest contacts, DPO details amended	Ian Headley
11th May 2018	2.0	GDPR review and updated to new legislation	Ian Headley
29th October 2019	2.1	Annual review, minor legislation references and contact detail change	Kelly Condon
3rd April 2020	2.2	DPA2018 reference change on police request form	Kelly Condon
17th January 2023	2.3	Annual Review	Kelly Condon

Table of Contents

Appendices

1. Purpose

1.1 UK Data Protection laws gives all individuals who are the subject of personal data ('data subjects') a right of access to the personal data that relates to them that the RNN Group (hereinafter referred to as the 'Group') collects and processes. These rights are known as 'subject access rights'. Requests for access to records and for other information about those records are known as 'data subject access requests'. Personal data may take the form of any electronic or paper records.

1.2 This document explains the rights of access to personal records and the procedures that must be followed to ensure compliance with UK Data Protection law.

2. Scope

2.1 This procedure applies to all members of staff who are approached to supply personal data about learners or members of staff or any other customers of, or stakeholders in the Group. These requests may come from the data subjects themselves, or external agencies such as, but not restricted to, the Police, Job Centre Fraud Investigation Unit, or the Department for Work and Pensions (DWP).

2.2 Additional information specifically relating to Data Protection within the Group is detailed within the Group Data Protection Policy and it is each member of staff's responsibility to ensure that they are familiar with same and have completed the mandatory Group Data Protection training to a satisfactory standard.

3. Definitions

3.1. Personal Data

3.1.1 The list provided below is not exhaustive but represents examples of the type of data that can be identified as 'Personal data' (as classified by the Group) this data can be described under the following terms:

a) Photographs.
b) Written personal details.
c) Video recordings.
d) Audio recordings.
e) Any combination of items that can be assembled to identify an individual.

3.1.2 Classes of information currently held by the Group may include, but are not restricted to:

a) Personal details.
b) Family, lifestyle and social circumstances.
c) Education and training details.
d) Employment details.
e) Financial details.
f) Details of goods or services provided.

3.2. Special Categories of Data

3.2.1 Special categories of personal data means personal data consisting of information as to:

a) Racial or ethnic origin.
b) Political opinions.
c) Religious or philosophical beliefs.
d) Trade union membership.
e) Genetic data.
f) Biometric data.
g) Data concerning health.

h) Data concerning sex life or sexual orientation.

3.2.2 Criminal offence data - The commission or alleged commission by an individual of any offence, or any proceedings for any offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of any court in such proceedings

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

3.3. Data Subject Access Request

3.3.1 A Data Subject Access Request (DSAR) is a request by an individual to see information held on them. The request can be verbal, written, via email or via social media and must be sent to the Information Governance and Assurance team (hereinafter referred to as the 'IGA team'). The request is only valid if the data subject can be identified. If there are reasonable doubts, then the IGA team will request further evidence to confirm the identity.

3.3.2 The IGA team must gather and provide all such information, on behalf of the Group, in a legible form where this is possible, without undue delay and within one month of the request being received. This data will be supplied without charge although there in certain circumstances and entirely at the discretion of the Data Protection Officer a charge may be levied, for example requests for large volumes of data.

3.3.3 A Data subject access request may also be made by a third party, with the express permission of the data subject, or for legal reasons such as the detection and prevention of crime, fraud investigations, legal enquiries, etc.

3.4. Exemptions and Redactions

3.4.1 Prior to being provided, information will be reviewed to confirm whether it can be released. In certain cases information will need to be redacted (for example to remove third party data) or refused under Article 23 of the GDPR, where an organisation can place exemptions on the rights of data subjects. Some of the exemptions that would prohibit disclosure in certain circumstances include:

a) The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

b) The protection of the data subject or the rights and freedoms of others

3.4.2 The Data Protection Officer will advise on whether an exemption request is justified prior to the request being processed.

3.4.3 Where third party information is present, then consent will be sought in order to release this or it will be redacted using Adobe Acrobat or other appropriate software which will permanently redact the data. Following redaction, the disclosure will be reviewed by the Data Protection Officer before it is released.

3.5. Data Subject Rights

3.5.1 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:

a) Transparent communication.
b) Information to be provided to the data subject e.g. controller details, DPO, third parties with access etc.
c) Information to be provided where personal data was not obtained from the data subject.
d) Right of access.
e) Right to rectification.
f) Right to erasure.
g) Right to restriction of processing.
h) Notification of rectification or erasure.
i) Right to data portability.
j) Right to object to processing.
k) Right to object to automated profiling decision making.

3.5.2 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.

3.5.3 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'.

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

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

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

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

3.6. Data Privacy Principles

3.6.1 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

3.6.2 The Group will not release any staff or learner data to third parties except to relevant statutory bodies, there is a statutory duty to do so, or where a relevant Group Data Processing Agreement is in place.

3.6.3 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 any personal data.

4. Responsibilities

4.1. The IGA team are responsible for dealing with all routine data subject access requests, without exception, and for the recording of such requests for the whole of the Group. The IGA team is also responsible for ensuring that data subject access requests are dealt with within the relevant timescales and in accordance with legal obligations, advising other staff in non-routine cases and for recording details of requests and outcomes.

4.2. All Group staff are responsible for their personal undertaking of the Data Protection training, this is mandatory within the Group and is a legal requirement.

4.3. Reference and/or attendance letters for learners are the responsibility of the Learner Recruitment and Reception Team within Learner Recruitment. Staff references are solely the responsibility of Human Resources.

4.3.1. Reference/Attendance letters for learners will be provided in line with the Group Learner Reference/Attendance Letter Procedure. Non-routine requests should be passed to the IGA team for action.

4.3.2. References for staff must only be supplied by Human Resources; any staff reference request should be directed to the Human Resources department in the first instance, without exception.

4.4. The Head of IT Services (or in their absence, the Deputy Head of IT Services) is responsible for advising on the management of data held on the Group's networks, the backups of same and cyber security.

4.5. The Learner Recruitment and Reception Team Leader is responsible for advising on, and ensuring any necessary training of the relevant staff regarding the supply of learner reference/attendance letters detailed above (4.3).

4.6. The Head of Student Support and Safeguarding (DDSL/Prevent Lead) is responsible for classroom contact if the Police or any other relevant statutorily entitled bodies apply for direct access to a learner.

4.7. Curriculum Managers are responsible for advising their staff on the process of DSAR's and ensuring that the Data Protection training is completed by their staff. They are also responsible for classroom contact if the Police apply for direct access to a learner for routine/general enquiries, in the absence of the Head of Student Support and Safeguarding (DDSL/Prevent Lead).

4.8. The Executive Director of HR, OD and Marketing is responsible for providing all staff related data to the IGA team when requested through the Group Subject Access Request process. The Director is also responsible for liaising with the Police if the nature of their enquiries and DSAR relates to a member of staff. See Appendix 1: Procedural Flowcharts - Flowchart 2, 3 and 4.

4.9. Senior Leadership Team (SLT) members are responsible for advising staff in non-routine cases, in the absence of the officers listed above and where the Police are seeking to apprehend an individual or individuals, learner or member of staff.

5. Procedure

5.1. General Data Subject Access Requests

5.1.1. 'Business as usual'. Examples could be a learner looking for their own ID number, or address or phone number to check if the information is correct. As long as you are sure of the individual's identity, this type of information can, and should be, supplied. No record needs to be kept for this type of transaction (See Appendix 1, Procedural Flowcharts, Flowchart 1: DSAR Procedure).

5.1.2. Information should only be released if the identity of the requestor and the appropriateness of release is without doubt. If there is any doubt, refer the matter to the IGA team. In general, information should not be released over the phone if this can be avoided, as the identity of the caller may be unclear.

5.1.3. Any data subject access request must be forwarded to the IGA team for recording and processing. (Appendix 2: Data Protection: Data Subject Access Request Form)

5.2. Police and External Agency Subject Access Requests

5.2.1. All Group Staff are entitled to ask to see a Police officer's warrant card for proof of identity and this can be recorded on the appropriate form.

5.2.2. When Police visit Group premises in person and request learner or staff data, if they do not hold a valid Police Force Data Subject Access Request Form, they MUST complete a Data Subject Access Request Form (Police) before any information can be supplied (Appendix 3: Data Protection: Data Subject Access Form (Police)).

5.2.3. If the enquiry is 'routine' and related to prevention and detection of crime, the information can be released. The completed Data Subject Access Request Form (Police) must be sent to the IGA team and will then be logged for compliance and record keeping purposes.

5.2.4. Due procedure must be followed if a Police officer asks to see a learner in person. See Appendix 1: Procedural Flowcharts, Flowchart 3: Police Data Subject Access Request – Access to learner or staff for routine/general enquiries and Flowchart 4: Police Data Subject Access Request - Subject arrest or detention in relation to serious crime for details.

5.2.5. If the enquiry relates to a serious crime, or the subject is likely to be detained or arrested then the matter MUST be referred to the Head of Student Support and Safeguarding (DDSL/Prevent Lead) (for learners), the Executive Director of HR, OD and Marketing (for staff) or in their absence, a member of the Senior Leadership Team of the Group. See Appendix 1: Procedural Flowcharts, Flowchart 4.

5.2.6. If advice is required, Group staff should contact relevant responsible managers as documented in Appendix 1: Procedural Flowcharts, or speak directly with the IGA team.

5.2.7. Enquiries from any other third-party organisations should be forwarded to the IGA team at sar@rnngroup.ac.uk for processing and recording.

6. **Linked Policies and Guidance**

Linked policies/related documents linked to this policy:

The RNN Group Data Protection Policy
Mobile Phone Policy
CCTV Policy
Procedure for Providing Learner Reference/Attendance Letters
Staff Acceptable Use Policy (AUP)
Learner Acceptable Use Policy (AUP)
The RNN Group Archiving Policy
The RNN Group Data Retention Policy
The RNN Group Privacy Policy
Data Breach Procedure

7. **Contact Details**

All Data Subject Access Requests (DSAR) enquiries, without exception, should be directed to sar@rnngroup.ac.uk in the first instance. These will be logged and forwarded to the responsible department or person for action accordingly.

Regulatory recording of enquiries, actions and outcomes are the responsibility of the IGA team and shall be centrally located.

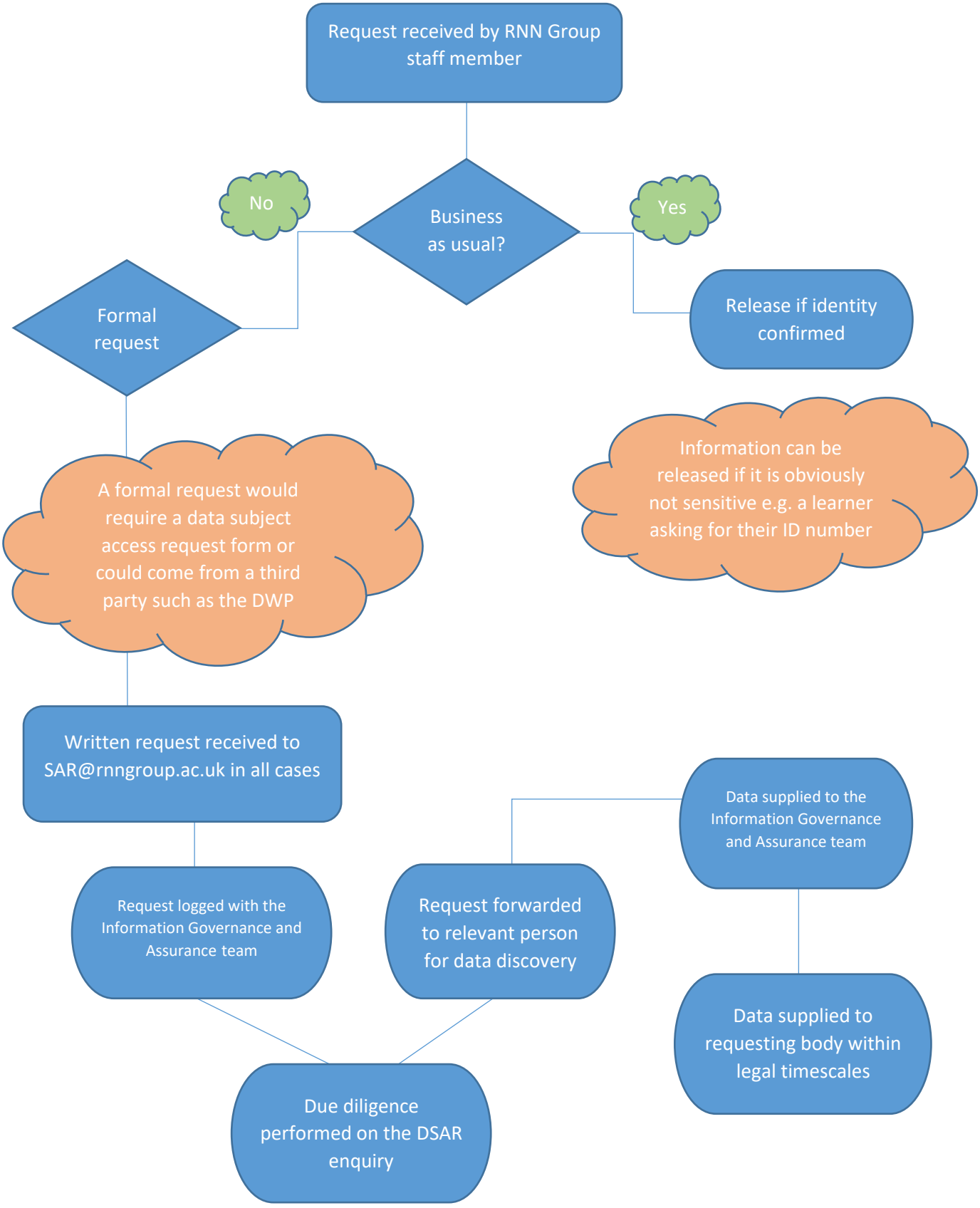
General Data Protection enquiries, not relating to DSAR's, should be directed to IG@rnngroup.ac.uk. This email address can be used internally and externally for enquiries of this nature.

If urgent contact is required for Data Protection issues, then the following numbers are to be used by staff and can be given out to individuals if the matter is requiring immediate attention:

IGA Team	-	01909 504666
Kelly Condon (Data Protection Officer)	-	07815 914809
Shamim Akhtar (Data Protection Advisor)	-	07773 313997
Ian Sutherland (Information Governance Assurance (Compliance) Officer)	-	07890 523646

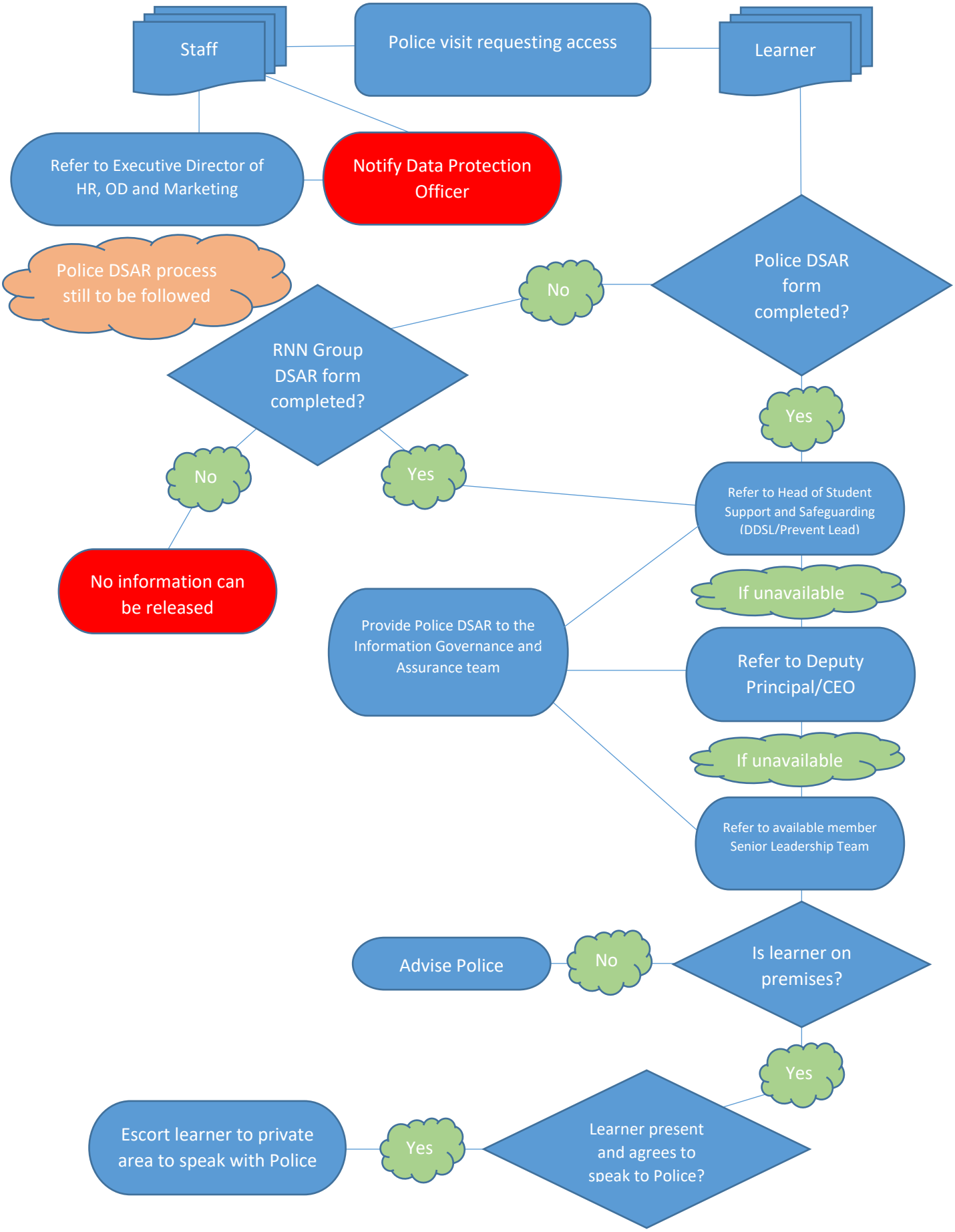
Appendix 1: Procedural Flowcharts

Flowchart 1: Data Subject Access Request (DSAR) Procedure

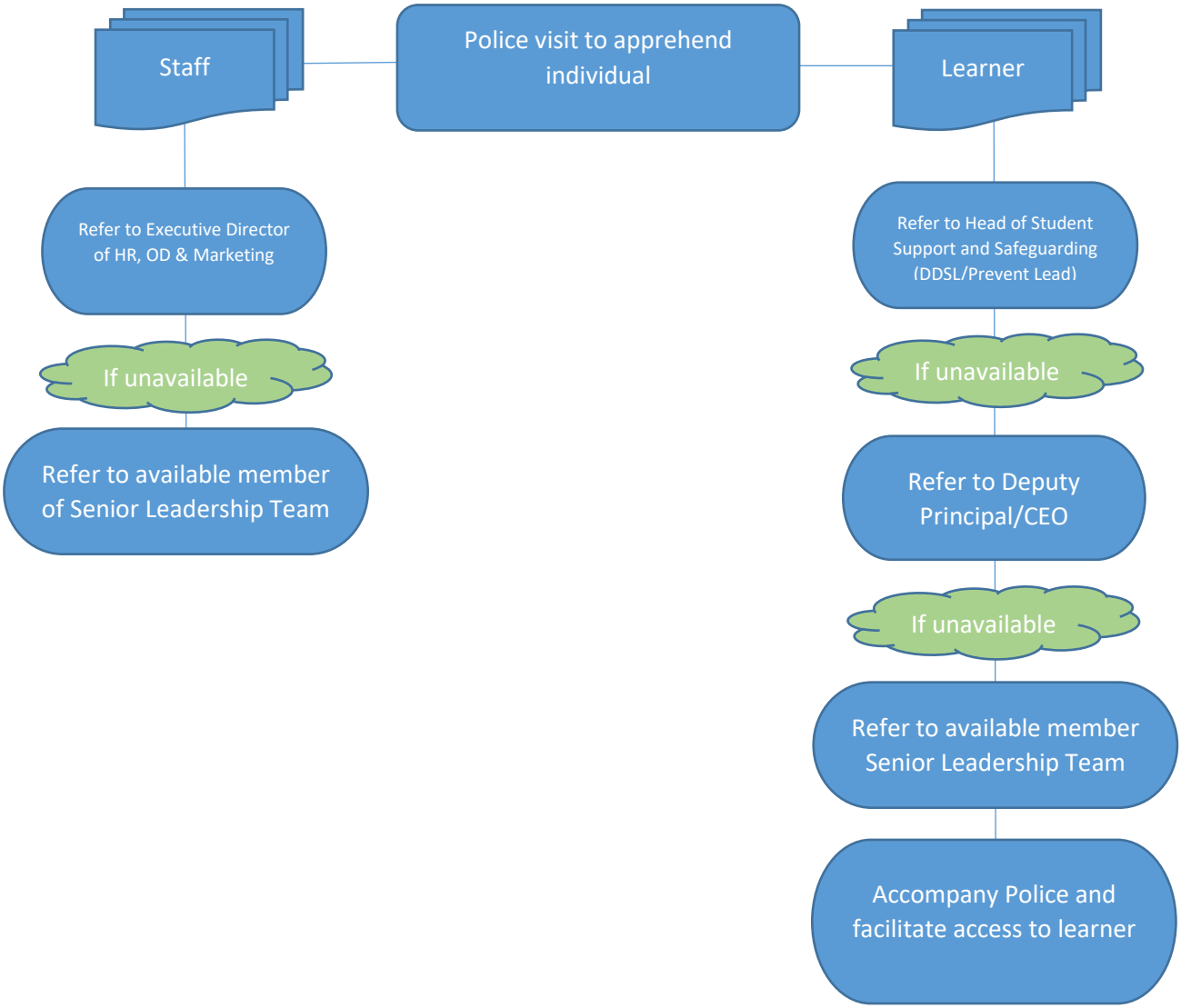


Flowchart 2: Police Data Subject Access Request Procedure – Information Only

Flowchart 3: Police Data Subject Access Request – Access to learner or staff for routine/general enquiries



Flowchart 4 – Police Data Subject Access Request – Subject arrest or detention in relation to serious crime



Appendix 2: Data Protection: Data Subject Access Request Form

Data Subject Access Request Form

Staff, learners (and other users of and stakeholders in 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 or on behalf of. 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.

Appendix 3: Data Protection: Data Subject Access Request Form (Police)

Data Subject Access Request Form (Police)

Police Reference:

RNN Group staff member name:

Date:

General Data Protection Regulations Article 23 (1) (d)

Data Protection Act 2018 Schedule 2 Part 1 Paragraph 2

I am making enquiries which are concerned with the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to, public security, in relation to:

Name of Data Subject:

Staff ☐ Learner ☐ Other ☐

Nature of enquiry
The information sought is needed to:

I confirm that the personal data requested is required for that/those purpose(s) and failure to provide the information will, in my view, be likely to prejudice that/those purpose(s).

Signed:

Rank/Number:

Name (BLOCK CAPITALS):

Contact Number:

Date:

Outcome/Details provided (RNN Group staff to complete)

Please Note: This form is only to be used in the event of an emergency i.e. when Police Officers have not been able to produce an original Police Force Data Subject Access Request Form to the relevant RNN Group staff member dealing with the initial request.

If the form is taken away from the RNN Group premises before final completion, Police Officers MUST forward a completed original form to the RNN Group after the site visit and prior to the release of any information.

RNN Group staff MUST make the Information Governance and Assurance team aware that the Police Officer has taken the form off premise for completion and advise of the Officer's number.

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

Appendix 4: Data Subject Access Request Form Process Flowchart