

GDPR Subject Access Request Procedure

UNCONTROLLED WHEN PRINTED

Version Control History

Version Number	Date of Change	Summary of Revisions Made
3.0	July 2015	Student Services Manager changed throughout to Head of Student Services. Information and Procurement Services Director changed to Acting Director of Corporate Services. Quality Manager changed to Head of Quality.
3.1	August 2016	Footer updated to reflect new template model. Role Title Change: Addition of Sector Manager
4	December 2016	Scheduled 2 – Yearly review identified the following minor changes: Paragraph 3.5 – New text inserted to highlight the right to consider motivation of any subject access request, particularly where we believe that servicing the request may be detrimental to the college. Paragraph 5.3 – Reference to access to staff email records, detailed in flowchart 5. Flowchart 5 added.
5	May 2018	Revision required to comply with GDPR Updated title of legislation. Updated number of days from 40 to 30. Updated to remove the charging element of previous legislation. Changes to job titles (SDDs). Changes need to be made to the job titles in the flowcharts but this is not critical at this stage as the persons are recognisable by these titles. Given that other job titles and responsibilities may change following the outcome of the restructure it is wise to leave this part of it for now.
5.1	December 2018	Change of role to Quality Manager. Updated footer.
5.2	March 2023	Rebranding

Data Protection Subject Access Request Procedure

1 Purpose

The General Data Protection Regulation came into force on 25 May 2018. It gives all individuals who are the subject of personal data ('data subjects') a general right of access to the personal data that relates to them. These rights are known as 'subject access rights'. Requests for access to records and for other information about those records are known as 'subject access requests'. Personal data may take the form of computerised or paper records.

This document explains the rights of access to personal records and the procedures that must be followed to ensure compliance with the General Data Protection Regulation 2018 (GDPR).

2 Scope

This procedure applies to all members of staff who are approached to supply personal data about students or members of staff. These requests may come from the data subjects themselves, or external agencies such as the Police, Job Centre Fraud Investigation Unit, or the Child Support Agency.

3 Definitions

3.1 **Personal data** is identified by the College under the following terms:

Photographs, written personal details, video recordings, audio recordings, and any combination of items that can be assembled to identify an individual.

Classes of information currently held by the College may include:

- Personal details.
- Images.
- Family, lifestyle and social circumstances.
- Education and training details.
- Employment details.
- Financial details.
- Goods or services provided.

3.2 **Sensitive Personal Data** means personal data consisting of information as to:

- The racial or ethnic origin of the data subject.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
- Physical or mental health or condition.

Title: Data Protection Subject Access Request Procedure

Version/Status: 5.2, Final

Approved By/Date: CMT/May/2018

Issue Date: March 2023

Owner: Chief Operating Officer

Lead Author: TBC

EQIA Approval Date: October 2016

- Sexual life.
- The commission or alleged commission by him/her of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

3.3 Subject Access Request

A Subject Access Request is a written, signed request from an individual to see information held on them. The Data Controller must provide all such information in a readable form within 30 days of receipt of the request. A subject access request may also be made by a third party, with the 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

There are exemptions built into the GDPR, and other laws can sometimes override the GDPR. Examples include the detection and prevention of crime and the use of the Child Support Regulations 1992, by agencies such as the Child Support Agency, which may override the GDPR.

3.5 Motivation

In certain circumstances, we are entitled to ask the data subject regarding the motivation for the request. If we believe that the data requested may be used in litigation or any other process that may be detrimental to the College, we can refuse to service the request, or parts of the request.

4 Responsibilities

- 4.1 College staff are responsible for dealing with routine subject access requests, and for recording of such requests. Staff are required to undertake mandatory Data Protection training. Non-routine requests should be passed to the Data Protection Officer.
- 4.2 The Data Protection Officer is responsible for ensuring that subject access requests are dealt with timeously and legally, advising staff in non-routine cases, and for recording details of requests and outcomes for an annual Board of Management report.
- 4.3 The Chief Operating Officer is responsible for management of Data Protection services and advising staff in non-routine cases, in the absence of the Data Protection Officer.
- 4.4 The Head of Student Experience is responsible for advising staff in non-routine cases, in the absence of the officers listed above. The Student Services Manager is also responsible for classroom contact if Police apply for direct access to a student.

Title: Data Protection Subject Access Request Procedure

Version/Status: 5.2, Final

Approved By/Date: CMT/May/2018

Issue Date: March 2023

Owner: Chief Operating Officer

Lead Author: TBC

EQIA Approval Date: October 2016

- 4.5 Sector Development Directors are responsible for advising staff in non-routine cases, in the absence of the officers listed above. They are also responsible for classroom contact if Police apply for direct access to a student, in the absence of the Head of Student Services.
- 4.6 Sector Managers and/or Subject Leaders are responsible for classroom contact if Police apply for direct access to a student, in the absence of Head of Student Services, or Sector Development Directors.
- 4.7 The Head of Learning and Teaching Enhancement is responsible for advising staff in non-routine cases, in the absence of the officers listed above.
- 4.8 Senior Management team (SMT) members are responsible for advising staff in non-routine cases, in the absence of the officers listed above, and where Police are seeking to apprehend an individual or individuals.
- 4.9 Quality approval check of the policy is the responsibility of the Quality Manager who will arrange for the policy to be published on the web.

5 Procedure

5.1 General Subject Access Requests

- 'Business as usual'. Examples could be a student looking for their own SQA 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.)
- Information should only be released if identity of the requestor and the appropriateness of release is clear cut. If in doubt, refer to the Data Protection Officer. In general, information should not be released over the phone, as the identity of the caller may be unclear.
- A formal request on a College subject access request form should be forwarded to the Data Protection Officer for recording and processing.

5.2 Police and External Agency Subject Access Requests

- When Police visit the College in person, if they do not hold a valid Police Force Subject Access Request Form, they **MUST** fill in a Subject Access Request Form (Police, Proforma) before any information can be supplied. (See Appendix 2.)

Title: Data Protection Subject Access Request Procedure

Version/Status: 5.2, Final

Approved By/Date: CMT/May/2018

Issue Date: March 2023

Owner: Chief Operating Officer

Lead Author: TBC

EQIA Approval Date: October 2016

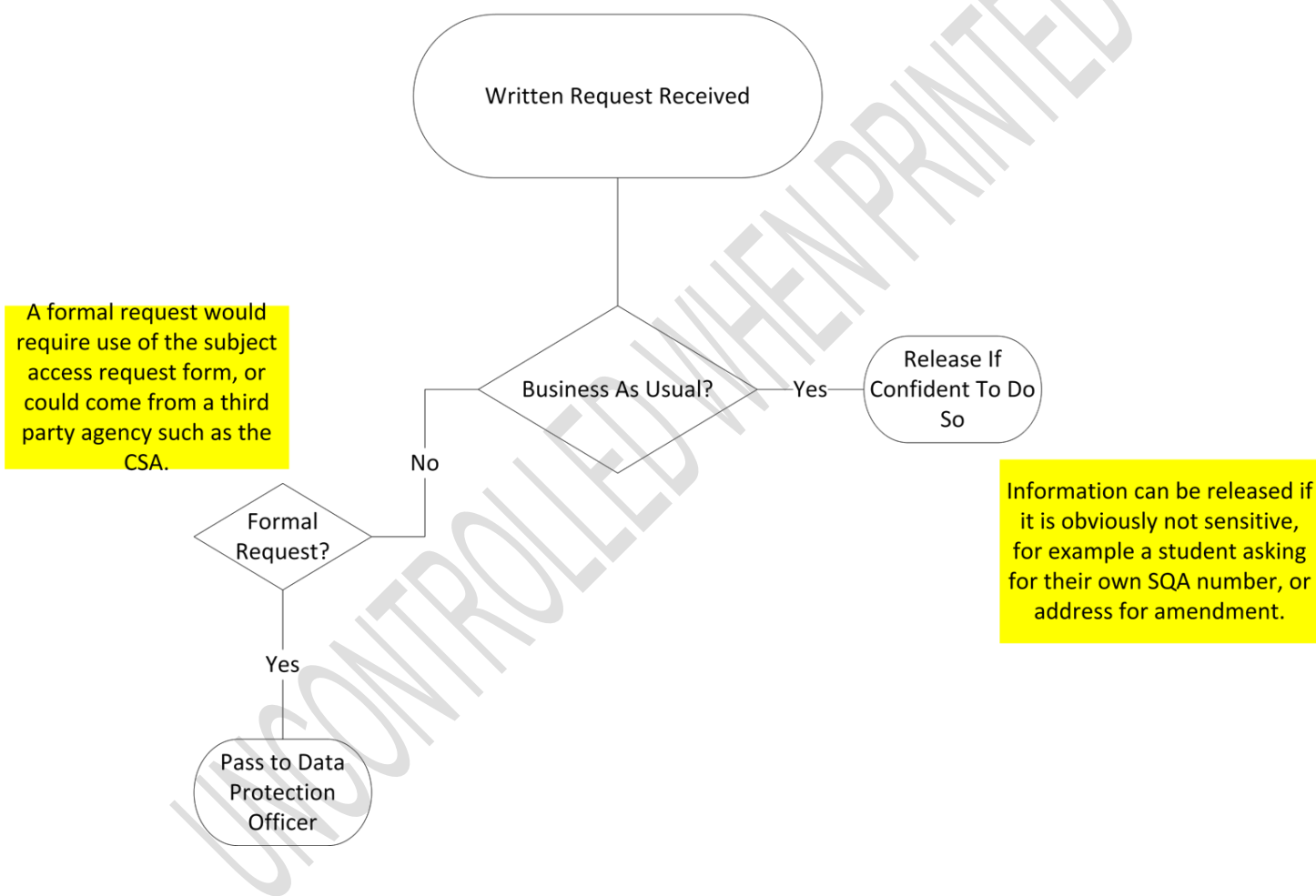
- If the enquiry is routine and related to prevention and detection of crime, the information can be released. Completed Subject Access Request Form (Police, Proforma) must be stored for compliance and record keeping purposes.
 - If the enquiry relates to a serious crime, or the subject is likely to be detained or arrested, the matter must be referred to a senior manager.
 - Staff are entitled to ask to see a police officer's warrant card for proof of identity.
 - Due procedure must be followed if police officers ask to see a student in person. See appendix 1 for details.
 - If advice is required, staff should contact relevant responsible managers as documented in Appendix 1: Procedural Flowcharts.
 - Enquiries from any other third party organisations should be forwarded to the Data Protection Officer for processing and recording.
- 5.3 For requests relating to email correspondence, refer to flowchart 5, accessing email correspondence.

6 Linked Policies/Related Documents

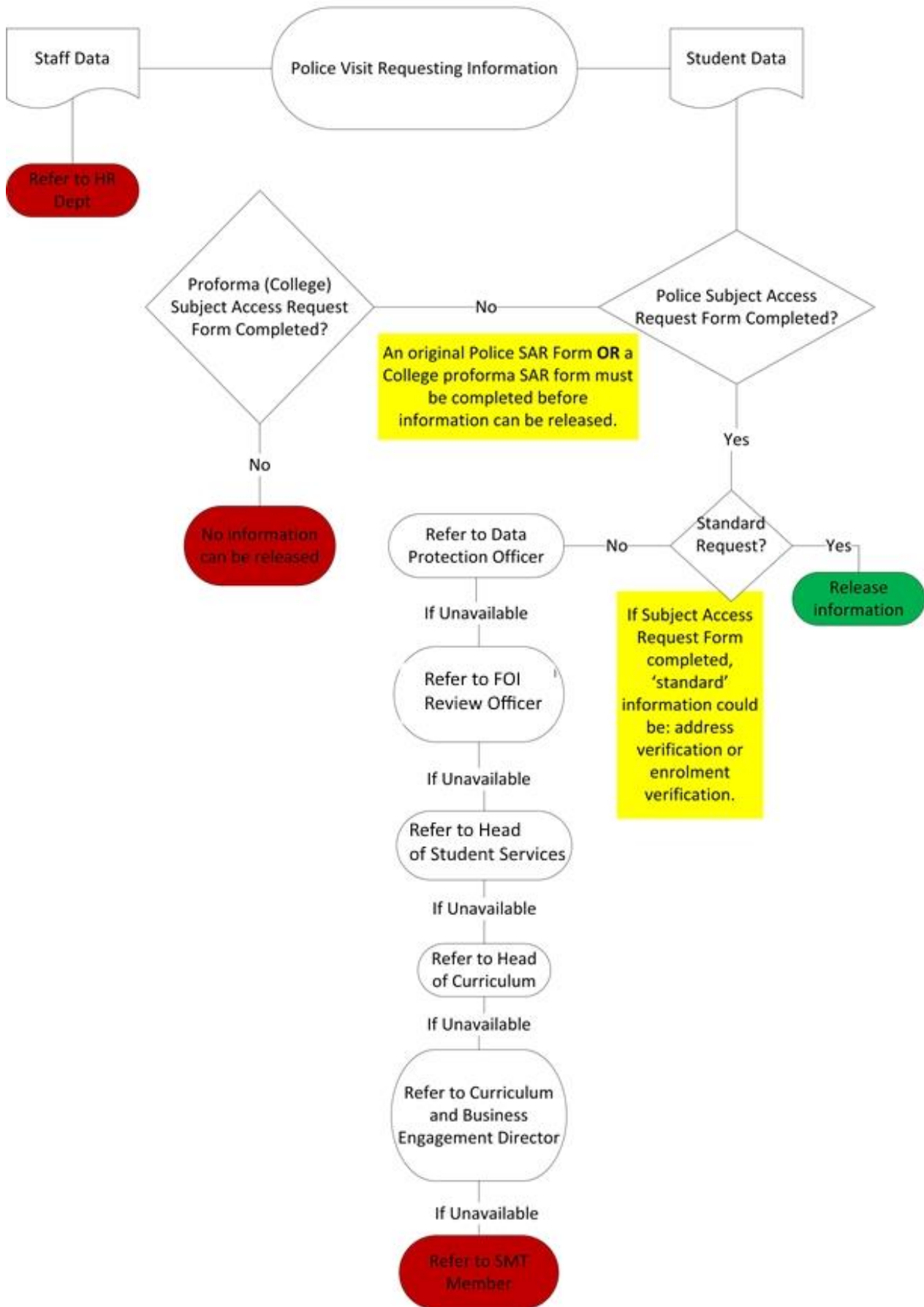
- 6.1 Data Protection Policy
- 6.2 Records Management Policy

Appendix 1: Procedural Flowcharts

Flowchart 1: Subject Access Requests Procedure



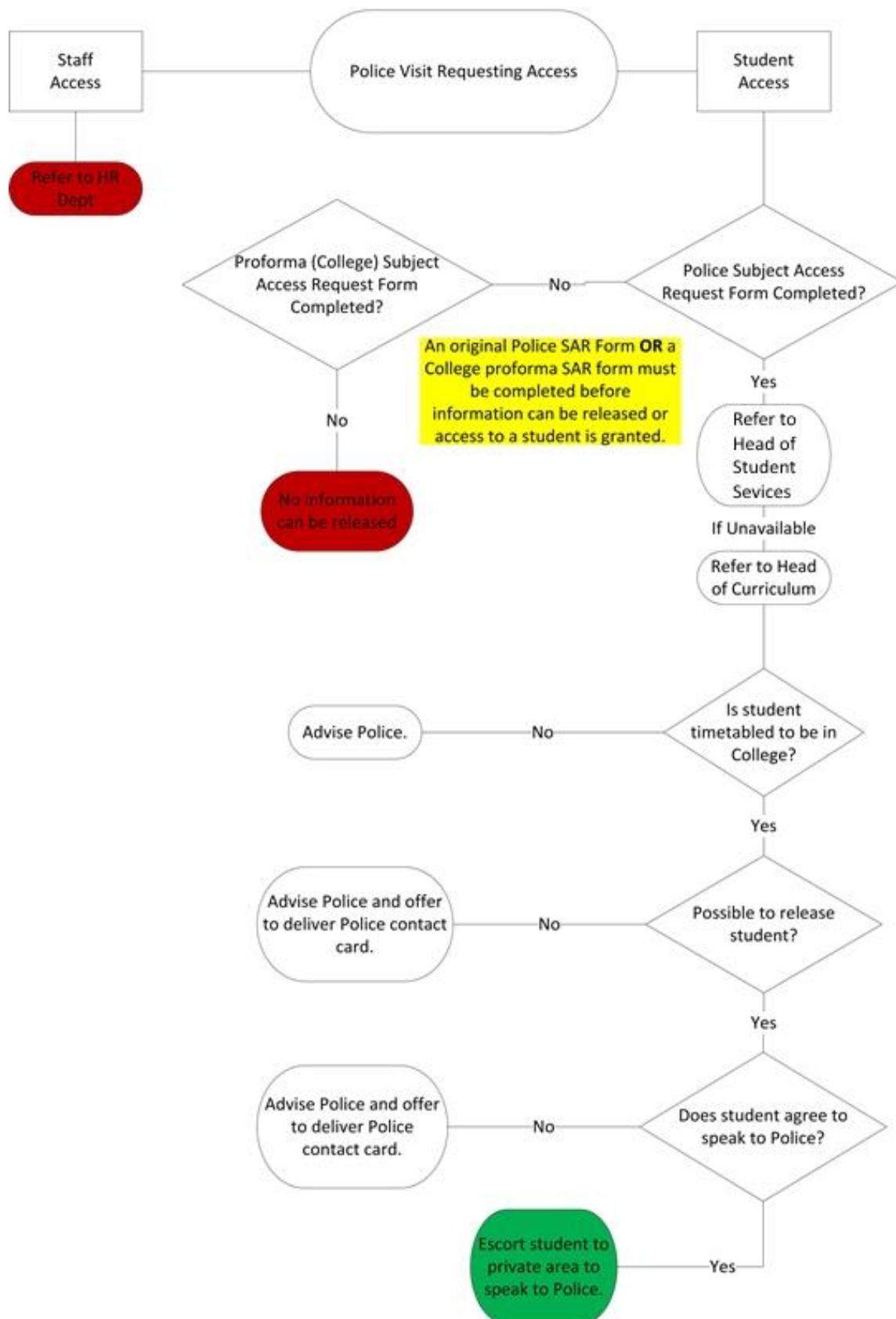
Flowchart 2: Police Subject Access Request Procedure Information Only



Title: Data Protection Subject Access Request Procedure
Version/Status: 5.2, Final
Approved By/Date: CMT/May/2018
Issue Date: March 2023

Owner: Chief Operating Officer
Lead Author: TBC
EQIA Approval Date: October 2016

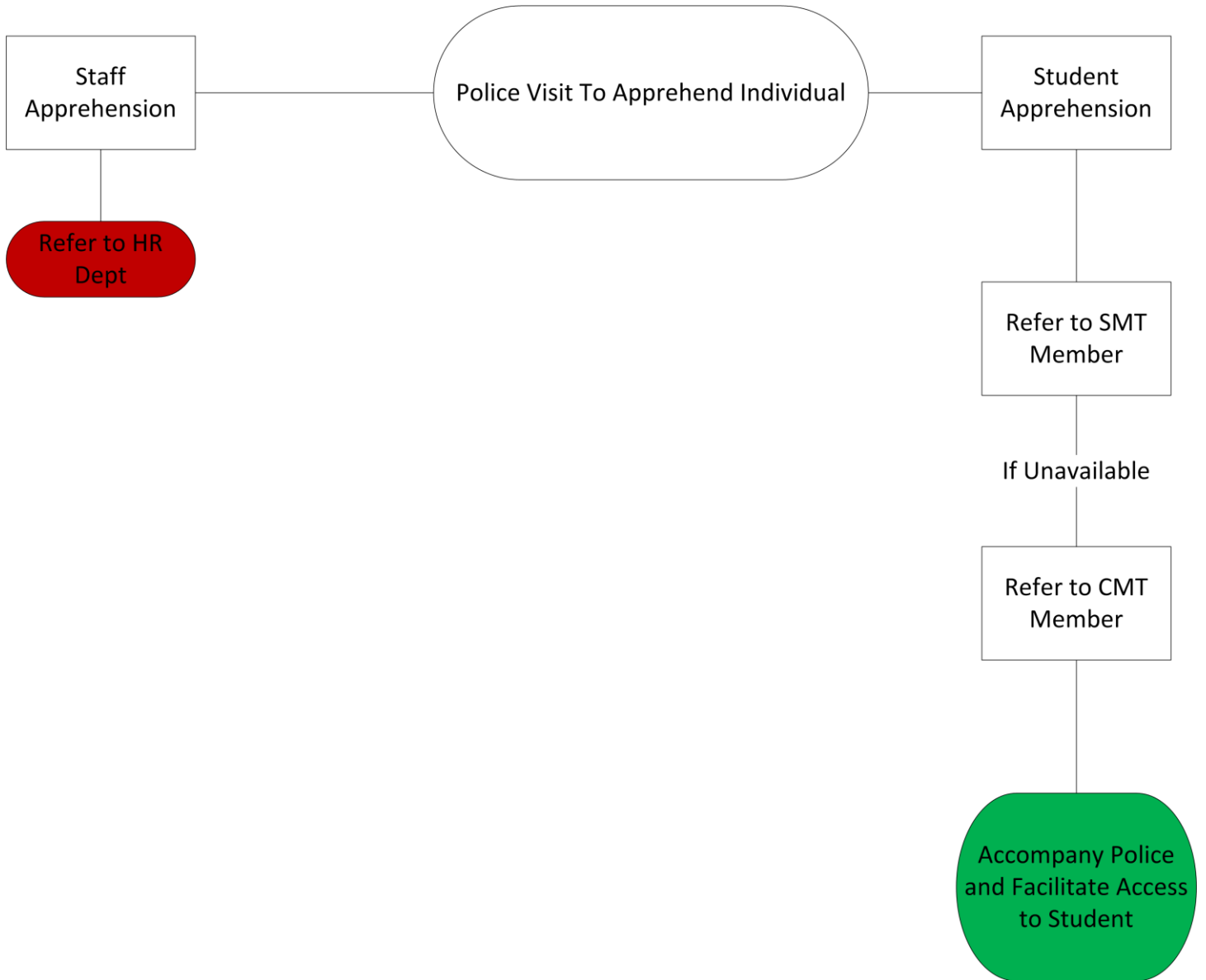
Flowchart 3: Police Subject Access Request - Access to Student or Staff Required for Routine/General Enquiries



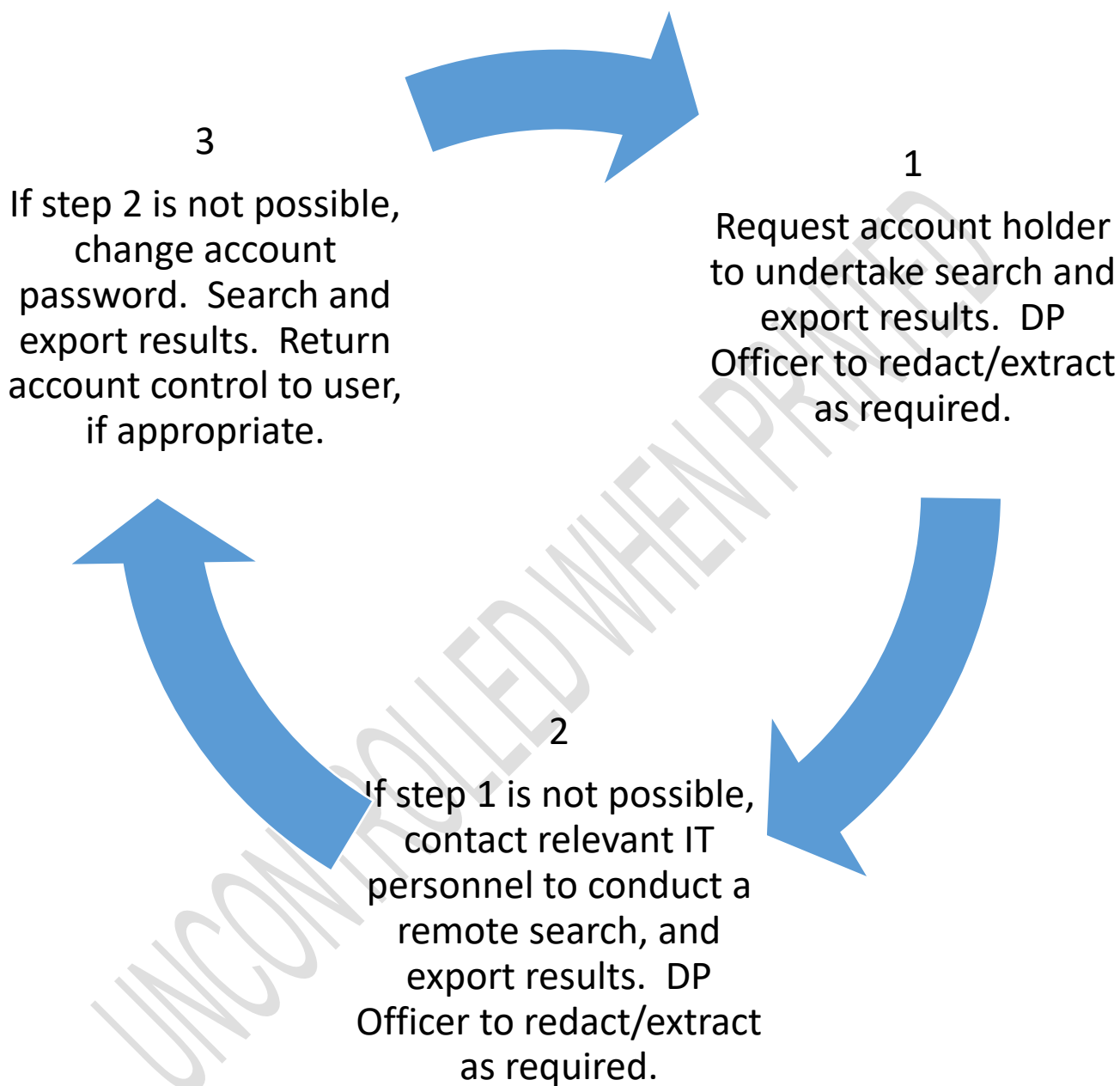
Title: Data Protection Subject Access Request Procedure
Version/Status: 5.2, Final
Approved By/Date: CMT/May/2018
Issue Date: March 2023

Owner: Chief Operating Officer
Lead Author: TBC
EQIA Approval Date: October 2016

Flowchart 4: Police Subject Access Request - Subject Arrest or Detention In Relation to Serious Crime



Flowchart 5: Accessing Email Correspondence



Appendix 2: Data Protection: Subject Access Request Form (Police, Proforma)

Police Reference: _____

Responsible Officer (College): _____

Date: _____

General Data Protection Regulation 2018

I am making enquiries which are concerned with:

- a The prevention or detection of crime.
- b The apprehension or prosecution of offenders.

Name of Data Subject:

Staff Student

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: _____

Date: _____

(BLOCK CAPITALS)

Outcome (College Staff)

Please Note: This form is only to be used in the event of an emergency, when Police Officers have not been able to produce an original Police Force Subject Access Request Form. Police Officers should forward a completed original form to Perth College UHI after the visit.

Title: Data Protection Subject Access Request Procedure

Version/Status: 5.2, Final

Approved By/Date: CMT/May/2018

Issue Date: March 2023

Owner: Chief Operating Officer

Lead Author: TBC

EQIA Approval Date: October 2016

Appendix 3: Data Protection: Subject Access Request Form

Under the terms of the General Data Protection Regulation 2018, staff, students and other users of the College have the right to access to personal data relating to themselves that is held by the College in electronic format and/or manual records forming part of a 'relevant filing system'.

Any individual who wishes to exercise this right should apply using this subject access request application form.

The College needs to be assured of an applicant's identity before relevant data is released.

The College may hold personal records in different parts of its organisation. To assist us to provide the information you require, please provide the following information:

Details Surname: Former Surname (if applicable): Forenames: Address: Telephone Number: Date of Birth:
Students Are you a present or past student of Perth College UHI? Yes/No (Delete as applicable) If yes, please give details of course of study and dates:
Staff Are you a present or past member of staff? Yes/No Present/Past (Delete as applicable) If yes, give department: For past staff, give dates of employment:
Others (Neither Staff nor Student) If you are neither staff nor student, please specify your connection with Perth College UHI:

Title: Data Protection Subject Access Request Procedure
Version/Status: 5.2, Final
Approved By/Date: CMT/May/2018
Issue Date: March 2023

Owner: Chief Operating Officer
Lead Author: TBC
EQIA Approval Date: October 2016

Information Required

The College may hold personal records in different parts of the organisation. Please specify the information you require. Please be as specific as possible to help us process your request as quickly as possible.

Your Signature: _____ Date: _____

On completion, this form should be sent to the:

Data Protection Officer
Perth College UHI
Crieff Road
Perth
PH1 2NX

College Use Only

Reference No: _____ Date Received: _____

Confirmation of identity checked: Yes No

Title: Data Protection Subject Access Request Procedure

Version/Status: 5.2, Final

Approved By/Date: CMT/May/2018

Issue Date: March 2023

Owner: Chief Operating Officer

Lead Author: TBC

EQIA Approval Date: October 2016