Data Subject Rights SOP

SOP Number:
246-05-2018

Academic Year:
2024/25 Onwards

Date Of This Issue:
April 2025

Responsible Owner and Enquiries:
Records Manager

Summary of Contents
In compliance with legislation and in line with the College Data Protection Policy this Standard Operating Procedure (SOP) provides staff with guidance in relation to actions they must take when data subjects exercise their Rights provided to them under the General Data Protection Regulations (GDPR).

RO Review Information:

First Created:	17 April 2018
Last Reviewed:	April 2025
Next Review:	May 2026

Change Type at last Review:
Minor

Approval/Noting By:
CMT: 17 April 2025

Previous Reference (for control purposes):
N/A

Date of Last Accessibility Screening:
April 2025

Contents

1.0 Change History

Changes to this SOP are documented in Appendix 1 of this document. When reading electronic copies of this document, you can click here to view the change history.

2.0 Background

2.1 SERC must process many categories of personal data to provide education, training and employment. It regards the lawful and correct treatment of personal information as imperative to successful operations and to maintaining confidence between all data subjects and ourselves. We ensure that our organisation treats information it processes lawfully and correctly.

2.2 The General Data Protection Regulations (UK GDPR) provides individuals with statutory Rights which can be exercised at any given time.

2.3 These rights are:

1. The Right to be Informed
2. The Right of Access
3. The Right to Rectification
4. The Right to Erasure
5. The Right to Restrict Processing
6. The Right to Data Portability
7. The Right to Object
8. Rights in Relation to Automated Decision Making and Profiling

2.4 The College must acknowledge and respond to all requests within the provisions of the regulations.

2.5 There may be occasions were an exemption, legal requirement or overarching business need applies which, in turn, restricts the extent of us meeting the data subjects wishes however all requests will be considered on a case-by-case basis.

2.6 All requests in relation to Data Subject Rights (DSR) must be processed and responded to without undue delay and in any event within one month of receipt of the request. In exceptional circumstances, the timeframe may extend by one additional month.

2.7 This SOP provides guidance on the process to be followed when a data subject makes a request in relation to his/her rights as per UK GDPR.

2.8 You must not destroy information as a result of an individual exercising their Rights. This is a criminal offence if it is done after a request has been made.

2.9 Exemptions to the format of the request may apply under the Disability Discrimination Act 1995.

3.0 Scope

3.1 Data Subject rights can be exercised by any individual whose personal data is processed by SERC.

3.2 In respect of an initial enquiry or receipt of a request this procedure applies to all SERC employees.

3.3 Once the request has been transferred to the Data Protection Officer (DPO), the procedures scope is limited to the DPO and data custodians.

4.0 Procedure

4.1 Receipt of a request

For the purposes of demonstrating accountability, transparency and good record keeping, the College would ask for all DSR requests to be submitted in written format. If an individual makes a verbal request the College will follow up in writing asking the individual to confirm our understanding and detail of what is being asked. Requests will not be actioned until confirmation from the requester has been received.

Requests may not be clearly identified as a DSR request. The requester does not have to quote UK GDPR or data protection to have the request treated as such.

Staff should consider if this is a legitimate request or a routine business enquiry and contact the DPO for guidance where there is uncertainty.

Once determined as a legitimate DSR request, it should be forwarded to the DPO who will assume responsibility for overseeing the request and providing a response.

4.2 Check that the request is within the scope of UK GDPR

Before proceeding with the request, the DPO will verify the following:

1. It provides sufficient information to verify the data subject's identity; and
2. It provides sufficient information to enable the College to locate, assess and action the relevant scope of the request.

4.3 Verify the identity of the data subject

Before processing the request, the identity of the data subject must be verified. Whilst it is important that you do not communicate personal information to people who are not the data subject, you must not appear obstructive. The College should take reasonable measures to verify their identity. You should keep a record of what measures you take.

You can often verify their identity from their circumstances, e.g. address, signature. If this is not possible, you can write to the individual asking them to send you a photocopy of some form of identification such as their passport or driving licence.

It is important to note if the data subject is making the request or is the request being made on behalf of the person. If a third party is making the request, you should only respond where there is a legal basis to do so. This will normally be 'consent' of the data subject.

There may be occasions where this measure is not required e.g. staff member making a request via their College email account.

4.4 Clarify the request

If the request is unclear or is very broad, you may contact the applicant to seek clarification or a reformulation of their request. This can be done by telephoning the applicant or in writing. For the purposes of recording the rationale behind how we respond to a request, it would be preferable to do this in writing.

Where further information is required before a search can be undertaken or a clear understanding of the request, the data subject should be contacted within 5 working days of receipt.

Where clarification is required the requester will be asked to respond within 5 working days from the date clarification is being sought.

The month deadline for response is re-calculated to begin from the date the clarification is received.

Seeking clarification must not be used as a means of allowing the College extra time to locate and review the information.

4.5 Calculate deadline for response

A response must be issued without delay and within a maximum time of 1 month from the date the request or clarification is received.

The due date for the response should be calculated. The calculation for the 'month' should be calculated as per date e.g. if a request is received on 4th March, the response should be received by the requester no later than 4th April.

4.6 Record DSR Request including:

1. The date the request is received must be recorded to evidence the timescale for response. The clock begins from the date of receipt by the College, not the DPO therefore it is imperative that confirmed or suspected DSR requests are forwarded to the DPO as soon as possible.
2. Input the request details on to the designated recording system.
3. Note the deadline for reply against the record.
4. Acknowledge receipt of request (The acknowledgement letter should be completed no later than 5 working days from receipt of the request).
5. All elements of each request must be recorded on the Subject Rights Request app to support actions taken, decisions, communications and guidance referred to.

4.7 Determine the information

How each DSR request is handled will depend on the category within which it falls. When searching for where personal information about the applicant might be held, you may need to search central filing systems, personnel records, and shared databases to locate the requested data. You may also need to speak to members of staff across different departments who might hold information about the individual.

The DPO, upon assessing the scope of the request, will contact the IT & Services department (IT&S) and arrange for a 'litigation hold' to be activated on the relevant systems to protect information within the scope of requests.

The College will operate a '3 option' method of extracting electronic information. The account holder will choose how they prefer the information to be extracted.

1. The account holder retrieves the information independently and declares to the DPO that all information held in relation to the request has been provided.
2. An IT&S department staff member retrieves the information in the presence of the account holder.
3. An IT&S department staff member retrieves the information remotely in the absence of the account holder.

If a conflict between individuals is made known to the DPO, the DPO will independently decide the most appropriate method to proceed with.

Staff who hold the requested information must declare everything which falls into the scope of the request. Information must not be deleted, or access obstructed to hinder the College meeting its legal obligation towards the Right's afforded by UK GDPR.

IT&S will audit relevant accounts to ensure all necessary information has been declared and report irregularities to the DPO.

The 'litigation hold' will be de-activated once the process of information extraction, response and appeal has been concluded.

The following is guidance however the DPO (or delegates) may operate discretion, flexibility and extra measures as each request will vary.

1. The Right to be Informed
    i. This request may be an individual asking questions such as how we are processing their data, why are we carrying out a certain processing activity, querying our legal basis or who their data may be shared with etc.
    ii. The College has a Privacy Notice on the website which individuals can be directed to. It will contain the broad, high volume or significant processing activities of the College.
    iii. For activities not included on the Privacy Notice, the DPO will contact the relevant Head of Department/School to determine the background to the processing.
    iv. There may be exemptions of a data subjects right to be informed e.g. where the processing is subject to criminal investigation. Such considerations will be reliant on thorough co-operation of all relevant staff.

2. The Right of Access
    i. Identify the individual's relationship with the College e.g. staff, student, customer as this will help identify where personal information about the applicant might be held and locate that information.
    ii. You may need to search relevant filing systems, personnel records and shared databases.
    iii. You may also need to speak to members of staff across different departments who might hold information about the individual.
    iv. It is imperative that the data custodians inform the DPO if there are risks associated with certain disclosures. The DPO can then determine if there is an existing exemption to protect the information.

3. The Right to Rectification
    i. The data subject has a right to ask for inaccurate information to be corrected.

ii. Once it is clear what information is being queried, the DPO should contact the lead custodian of that data.

iii. Consideration should be given by all parties involved as to the scope of the request i.e. does the information stretch beyond one department, are third party processors involved and if so, they should also be notified.

iv. There may be occasions where the information cannot be changed however a note may be put against the data to reflect the inaccuracy.

4. The Right to Erasure

i. This Right may be more commonly recognised as the 'Right to be Forgotten' and may be referred to as such by the requester.

ii. If the data subject has reason to believe their information is being processed without a legitimate basis, they may ask for the data to be deleted or removed.

iii. In some circumstances the College may have an overarching business need to either partially delete the data or not at all. Such cases may include:

   a. We have a legal obligation to retain the information

   b. Public interest is better served by keeping it on record

   c. Information is required to substantiate or refute a legal claim

iv. Consideration should be given by all parties involved as to the scope of the request i.e. does the information stretch beyond one department, are third party processors involved and if so, they should also be notified.

v. The DPO and data custodians must consider the impact of erasure and together record the rationale behind the final decision.

vi. Regardless of the final decision, the DPO will either confirm deletion or communicate our rationale for our need to keep the information active.

5. The Right to Restrict Processing

i. This Right allows individuals to request a halt on the processing of any personal information which they consider to be inaccurate, unlawful or to defend or refute a legal claim and they do not wish for the data to be deleted.

ii. This list is not exhaustive and all requests should be considered.

iii. The DPO and data custodians must look at the areas where the information is processed e.g. departments, systems, files

iv. The College will be permitted to retain the data, but further processing will not take place.

v. We will also keep a record of information to ensure this Right is respected in future processing by our organisation.

6. The Right to Data Portability

i. An individual who registers with another service provider may request that their information is transferred to them directly.

ii. The right to data portability only applies:

   a. to personal data an individual has provided to a controller.

b. where the processing is based on the individual's consent or for the performance of a contract; and

c. when processing is carried out by automated means.

iii. The DPO should contact the data custodian, this will primarily be I.T to determine the process required to meet this request.

iv. Information may be electronically transferred to the third party safely and to the point of being re-used by them.

v. We will provide the personal data in a structured, commonly used and machine-readable format. Machine readable means that the information is structured for software to extract specific categories of information. The new service provider should in turn, be able to re-use the information we have provided to them.

vi. We may be able to transmit the data directly to another organisation if this is technically feasible. This will be considered on a case-by-case basis depending on the software available to both parties.

7. The Right to Object

i. If an individual believes our public task is unfounded or they wish to have their details removed from direct marketing campaigns or research/statistical processing, this Right gives them the opportunity to object to these processing activities.

ii. Processing for performance of a legal task or Public Authority purpose:

a. We will grant your request unless there is a legal basis to continue the processing or if the processing is to settle a legal claim.

b. This legal purpose can be confirmed with the data custodian

iii. Rights in Relation to Direct Marketing:

a. If an individual wishes for their details to be removed from our marketing lists, we will comply with your request immediately and no further advertising should be issued by the College to that individual.

b. These requests must be communicated to Marketing immediately and mailing lists updated with this new preference.

c. List of subscribers and mailing preference lists should be refreshed immediately prior to every advertising communication.

iv. Rights in relation to statistical/research purposes:

a. If the College has reason to process personal information for this reason, we will consider all requests and where possible grant your request unless it is necessary for the performance of a public task.

8. Rights in Relation to Automated Decision Making and Profiling

i. If personal information is subject to automated decision making i.e. there is no human involvement, individuals have a right to ask for a person to review the information and make a fresh decision.

ii. The College cannot guarantee a different outcome, but human intervention may explain rationale to the individual.

iii. There are some instances where this Right does not apply, such as:

a. The processing is necessary for contractual purposes
b. The processing is based on consent

Further guidance on all such Rights is available on the ICO website ***www.ico.org.uk***

4.8 Review information considering possible exemptions:

1. Once you have identified the location of all information, you must consult with the data custodian and other relevant managers to discuss the impact of the request e.g. can we erase all data, is there a legal basis for processing which prevents erasure, what is the impact of disclosure.
2. If the request relates to disclosure and the College considers this a risk, you must consider any relevant exemptions in legislation.
3. This must be done on a case-by-case basis for each individual piece of information. In some cases, you may be able to action elements of a request, but not all.
4. If you are being asked to disclose information, only that which is about the person making the request should be released. You should redact personal data of any third party if a legal basis to process does not exist. Redaction should result in third parties being unidentifiable. Guidance on anonymisation is available in the FE Sector GDPR Handbook and the Information Commissioners Office (ICO) website.

4.9 Responding to the Applicant

The applicant should receive a response in permanent form without delay and within a maximum time of 1 month from the date the request or clarification is received

If the request relates to Right of Access, the requester must be provided with the following in the response:

1. Confirmation if personal data is being processed
2. Access to that data, where exemptions do not apply
3. Purpose of processing
4. Categories of data concerned
5. Recipients to whom the data is shared
6. Retention period of the data, where possible
7. existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
8. the right to lodge a complaint with the ICO
9. where the personal data are not collected from the data subject, any available information as to their source
10. the existence of automated decision-making, including profiling

In relation to all other Rights requests, the individuals should be provided with either a confirmation that their request has been actioned or an explanation as to why the College is unable to process their request.

4.10 Example Response Letter:

Dear **XXX Customer Name XXX**

Thank you for your request received by the College on **XXX Insert Date XXX**. Your request was considered in line with the General Data Protection Regulations and Data Protection Act (2018) which provides you with the Right of Access to information concerning you.

In your request you asked for the following:

- **XXX Provide details of request in bullet form XXX**

Please find attached the information which you have requested. The password will be forwarded separately. **XXX Responder may wish to issue information via One Drive rather than attach XXX**

XXX provide details of exemptions applied, redactions etc XXX.

Your Right to Appeal

If you are not happy with how the College has handled your request or exemptions applied to the response, they have a right to ask for an internal review of their request. Appeals should be submitted within 10 working days of receipt of this response detailing reasons for dissatisfaction and should be addressed to:

✉ **Data Protection Officer**
SERC Bangor Campus
Castle Park Road
Bangor
BT20 4TD

informationright@serc.ac.uk

XXX Insert signature including title and correspondence details XXX

5.0 Appeals Process

5.1 If a requester is not happy with how the College has handled their request or exemptions applied to the response they have a right to ask for an internal review of their request. Appeals should be submitted within 10 working days of receipt of this response detailing reasons for dissatisfaction and should be addressed to:

✉ **Data Protection Officer**
SERC Bangor Campus
Castle Park Road
Bangor
BT20 4TD

informationright@serc.ac.uk

5.2 The DPO will issue an Appeal acknowledgement within 5 working days from receipt of appeal.

5.3 The DPO will convene a panel of independent personnel who will then examine the initial request/response, the request for appeal and review if there are areas for improvement and whether or not the College should reconsider its original response rationale.

5.4 The College will issue a response to all appeals within 20 workings days from date of the acknowledgement letter being issued.

5.5 A working day is any day other than a Saturday, Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom. A 'working day' is considered to end at 23:59.

5.6 If the requester is not happy with the Appeal Panel decision, they may contact the Information Commissioners Office (ICO) with a 'request for assessment' at:

ICO
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

6.0 Recording All Requests

Each request should be fully documented with the following:

1. Name/contact details of the requester
2. Nature of the request
3. Date request received/responded to
4. Copies of all correspondence between the College, the data subject and any other parties

5. A record of any telephone conversations used to verify the identity of the individual or the information required
6. A record of your decisions and how you came to make those decisions e.g. application of exemptions
7. If redactions have been made, copies of unredacted info should be retained; and
8. Copies of information sent to the data subject.

7.0 Communication Plan

7.1 This Procedure will be uploaded to the College intranet and referred to in staff induction and training.

7.2 All staff to receive awareness raising and training to demonstrate an understanding of the requirements and responsibilities of the Freedom of Information legislation.

8.0 Review

8.1 This SOP will be reviewed annually or sooner if required to reflect changes in legislation, circumstance or procedure.

Appendix 1: Document Change History

Version	Date	Change Detail
1.1	July 2021	4.5 added: A working day is any day other than a Saturday, Sunday, Christmas Day, Good Friday or a day which is a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom. A 'working day' is considered to end at 23:59.
1.2	August 2022	No Changes Required
1.3	July 2024	Transferred to Accessibility Template
1.4	April 2025	No Significant Changes Required