Document Control

Title	Data Subject Access Procedure
Primary Author(s)	Information Governance
Related Policies	Data Protection Policy, Information Governance Framework
Accountable Authority	SIRO
Approving Authority	Head of Information Governance
Date of Approval	N/A
Date of Review	As needed

Version History

Version	Date Issued	Author(s)	Notes
1.0	01/03/2023	Information Governance Team	Initial version
1.1	06/03/2024	Information Governance Team	Revisions
1.2	28/05/2025	Information Governance Team	Revisions to 3.2, 3.3, and 5.5
1.3	12/02/2026	Information Governance Team	Additions and Revisions to 5.16-19 and 5.21-27

1 Purpose

1.1 The General Data Protection Regulation (GDPR) provides data subjects with a number of data rights as outlined in the University's Privacy Notices, including the right of access. A Subject Access Request (SAR) is a means by which an individual finds out what Personal Data an organisation holds about them, why it is held, and with whom it is shared.

1.2 This Procedure sets out how individuals can make a request and how the University identifies and manages its SAR responsibilities in accordance with its legal and regulatory obligations.

2 Definitions

2.1 **SAR** – Data Subject Access Request, a legal obligation whereby individuals have the right to copies of their personal data held by the University in any recorded format, including in mailboxes, teams channels and OneDrive.

2.2 **FOIA Requests:** Requests made to the University under the Freedom of Information Act 2000, giving the public the right to be given information held by the University, which can include correspondence between staff members, information held in emails, teams and OneDrive**.**

3 Scope

3.1 This procedure applies to all University of Southampton staff, students and authorised third parties, including but not limited to temporary and agency staff, visitors, contractors, interns and volunteers (Users) who process Personal Data.

3.2 The procedure is also applicable for all data subjects making a request to the University for their personal data, except for requests for dyslexia assessments.

3.3 Current and former students requiring copies of dyslexia assessments and reports should apply directly to the Student Hub at sedcen@soton.ac.uk Any requests for such reports received by the Information Governance Team will be redirected to the Student Hub.

3.4 Individuals wishing to request information held by the University other than their own personal data should refer to the University's FOIA procedure and webpages.

4 Principles

4.1 The University's Data Protection Policy outlines the University's position in relation to its obligations under the Data protection legislation and associated regulations.

4.2 A SAR may be received by anyone at the University, but it should be managed by the Information Governance Team.

4.3 The University must respond to a SAR within set timeframes as part of compliance with the law, therefore all University staff should be aware of what a SAR is, have a general understanding of what the University's obligations are to comply with such a request, and specific knowledge of their role and responsibilities in relation to a SAR.

4.4 The right of access gives individuals the right to obtain a copy of their personal data as well as other supplementary information. Personal data may include, but is not limited to, information held within staff files, student record files, databases, interview notes, and e-mail correspondence which refers to the individual.

4.5 A Data Subject's right to see their personal data shall not adversely affect the rights and freedoms of other people. Where third party individuals are likely to be impacted, reasonable efforts will be made to notify those individuals.

5 Procedure

5.1 A SAR can be made verbally or in writing, including on social media. A request is valid if it is clear an individual is asking for their own Personal Data. If a staff member is made aware of such a request, they must either refer the individual to the University's online form or forward the request to the Information Governance Team at data.protection@soton.ac.uk

5.2 Individuals can submit a request directly to the Information Governance team by completing the University's online form or by emailing data.protection@soton.ac.uk

5.3 The University is required to communicate to the data subject request with the information it holds in an intelligible form without undue delay or at the latest within one month of receipt of a valid request (including verification).

5.4 In the case of very large or complex requests, the University may (under article 12(3) UK GDPR) extend the deadline for compliance by up to a further 2 months. In these cases, the Information Governance Team must inform the data subject of the extension within 1 month of receipt of the request.

Verification

5.5 Individuals submitting a request must provide identification to enable the University to verify the individual. Where such identification is not included with the initial request the Information Governance team will ask for this to be provided within 7 days of acknowledging the request. If proof of identification is not provided within this time limit, the request will be closed and the individual will be able to make a new request, with their proof of identification. The statutory timescales for response will be calculated from the date on which satisfactory proof of identification is received.

5.6 Suitable forms of ID are photo identification such as passport, driving licence, or, if the request is being made by a student, alumni or staff member their identity will be confirmed through their use of a University email account.

Review

5.7 The Information Governance Team will assign a reference number to the request and issue an acknowledgement (with a request for identification, if applicable) to the requester.

5.8 A broad request, such as a request for "everything" or a request for "all emails that refer to or mention me" is usually likely to be excessive or unfeasible to undertake. In these circumstances the Information Governance Team will seek clarification or further detail from the individual requester if the request is too broad to be reasonably fulfilled within statutory timescales.

5.9 Once the request is confirmed, the Information Governance Team will conduct the necessary searches and exports of relevant files and networks to retrieve the information.

5.10 Where the information requested is located in a staff email account, whether individual or generic mailboxes, or in individually owned network locations, the email or folder's owner will normally be contacted to assist with the request. Where the request is for a significant volume of information (such as multiple search terms or over a significant period of time) the Information Governance Team will retrieve the information centrally in line with the University's Data Access Procedure.

Collation

5.11 Information Governance will collate the information applicable to the scope of the request and undertake checks and necessary redactions before finalising the disclosure.

5.12 Redactions will be applied on the basis of any applicable exemptions, and the disclosure will include detailed explanation of all redactions and the rationale behind them.

5.13 For the cohesion of the disclosure, redactions will usually be applied on an exceptional basis where exemptions apply, and therefore the disclosure may include information already known to the data subject (such as emails they have previously received) however efforts will be made to remove duplicates where this will not impede clarity.

5.14 Disclosures will usually be presented in a single pdf format, with OCR (optical character recognition) to enable the disclosure to be searched by the requester

5.15 Disclosures are sent to the requester via the University's file sharing software SafeSend and will be encrypted. The password will be sent to the requester under a separate email.

Relationship with Other University Procedures

5.16 The Subject Access Request process is a statutory process under data protection legislation and operates independently from any other University procedures, including but not limited to disciplinary, grievance, complaints, fitness to practice or appeal processes.

5.17 The existence of an ongoing or concluded University procedure does not remove an individual's right to submit a SAR. However, a SAR is not the appropriate route to follow if the intended disclosure will be used to supersede, circumvent, replace, or interfere with established procedural disclosure routes. The timing, scope or content of a SAR disclosure will not be aligned to influence or support any ongoing procedure, in particular where such a procedure will result in disclosure of the same information. The only interaction between a SAR and an ongoing procedure will be limited to the consideration of lawful exemptions and appropriate redactions, including where disclosure could prejudice the rights and freedoms of others or the integrity of University processes.

Refusing a Request

5.18 Data subjects are entitled to access their own personal data only. Information may be redacted or withheld where an exemption under the Data Protection Act 2018 applies, including where disclosure would adversely affect the rights and freedoms of others.

5.19 Exemptions may apply to protect particular categories of information, confidential references, legally privileged material, management forecasting or planning, or information relating to third parties where the University owes a duty of confidence.

5.20 The University may refuse a SAR if:

An individual is asking for personal data about another individual or the information which they are requesting contains personal data about another individual, unless:

- the second individual has also given permission for that user to be able to access that information.
- It is reasonable for the University to provide data about a different individual without their consent.

5.21 The right of access does not require the University to provide copies of personal data which is already reasonably accessible to the data subject. This may include, but is not limited to:

- Information already provided to the individual through routine University processes.
- Information available to the individual through secure systems or portals to which they have authorised access.
- Documentation that will be disclosed to the individual as part of a concluded University procedure, such as the outcome of a disciplinary, grievance, complaint or appeal process.

In such circumstances, the University may withhold this information from a SAR response and will explain the basis on which it is considered reasonably accessible.

5.22 The University may refuse to comply with a SAR where it is considered to be manifestly unfounded or manifestly excessive, in accordance with Article 12(5) UK GDPR. In such cases, the University will be able to demonstrate and document the justification for refusal.

5.23 When assessing whether a request is manifestly excessive, the University will consider all relevant factors, including but not limited to:

- The scope, breadth and complexity of the request.
- The volume of data requested, and the number of systems or locations required to be searched.
- The disproportionate use or current capacity, of University resources required to comply with the request.
- Whether the request repeats previous requests without a reasonable interval or justification.
- Whether the request overlaps significantly with information already disclosed or reasonably accessible to the data subject.

5.24 A request may be considered manifestly unfounded where it is evident that the SAR is being used for purposes unrelated to the right of access, including where it is being used to attempt to obtain early or enhanced disclosure of documentation outside of established University procedures.

5.25 This may include, for example, circumstances where a data subject submits a SAR during an ongoing disciplinary, grievance, complaint or appeal process with the

intention of accessing documentation in advance of procedural disclosure stages or deadlines.

In such cases, the University will assess the request on its merits and may refuse the request where it can be demonstrated that the primary purpose is to undermine or bypass the relevant procedure rather than to exercise data protection rights.

5.26 Where the University refuses to comply with a SAR, in whole or in part, it will inform the data subject without undue delay, explaining the reasons for the refusal and their right to lodge a complaint with the Information Commissioner's Office or seek a judicial remedy.

6 Third Party Requests

6.1 The University may receive requests via third parties, such as solicitors, or other representatives. In such cases, the University will require a letter of authorisation from the data subjects, together with proof of their identity.

6.2 The request is then processed in accordance with the procedure outlined in section 5.

6.3 Where requests for information received by other third parties, such as law enforcement, statutory bodies like the Disclosure and Barring service or other relevant bodies; the request will be dealt in line with section 5 of this procedure and the Data Access Procedure with the following exceptions:

- Request will be verified, either through a phone call, checking the contact details provided and reviewing the DP2 (where a request is made under the general crime and taxation exemption)
- The request may be dealt with by other departments of the University, usually Student Support in urgent cases, or cases related to ongoing wellbeing or safeguarding concerns. In these cases a brief on the disclosure will be shared with the Information Governance team, including, where applicable, the retrospective DP2 form outlining the requirements and lawful basis for the information.

6.4 It is important to note that a request from these bodies will not automatically be carried out, and the Information Governance Team will assess requests to ensure that any data shared is done so in compliance with the Data Protection legislation. This will include proportionality, necessity and lawfulness and our obligations to notify individuals.