



Nottingham Trent
University

Governance and Legal Services

Subject Access Request Policy and Procedure

Version: 2

Date: August 2022

Version: 01
Date: April 2018
Approval: UET
Author: DPO
Next Review: 2021/2022

Version: 02
Date: August 2022
Author: DPO
Amended to reflect UKGDPR
and update procedure
Next Review: 2024/2025

Contents

1.	Introduction.....	2
2.	Scope and Definitions.....	2
2.1	Definitions	2
3.	Regulatory Requirements	2
4.	Responsibilities.....	3
4.1	University Executive Team (UET)	3
4.2	Employees	3
4.3	Legal Services and Data Protection Officer (DPO)	3
5.	Subject Access Requests (SAR).....	3
5.1	Purpose	3
9.1	Validity	3
5.3	Verification	3
5.4	Fees.....	3
5.5	Personal Data Released	4
5.6	Response Times / Seeking Clarification	4
5.7	Refusing a SAR	5
6.	SAR Procedure.....	5
7.	Minimum Standards.....	6
8.	Records Management	6

1. Introduction

The UK General Data Protection Regulation (UK GDPR) gives you the right to find out, and obtain a copy of, any information an organisation holds about you. 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.

This Policy and Procedure sets out how Nottingham Trent University (NTU) identifies and manages its SAR responsibilities in accordance with its legal and regulatory obligations. This Policy sets out the minimum standards which must be complied with by NTU.

See NTU's [Data Protection Policy](#) for an explanation of what is meant by "Personal Data" and "Special Category Personal Data", and what "Processing" Personal Data means.

2. Scope and Definitions

This Policy and Procedure applies to the entirety of NTU employees, students and where appropriate third parties working for, or on behalf of, NTU. This applies to all data relating to identifiable individuals throughout NTU and beyond.

2.1 Definitions

Data Subject	Individual who NTU holds Personal Data about.
Personal Data	Information which relates to a Data Subject and which is identifiable to them.
Corresponding Information	Information relating to the processing of Personal Data, which is usually contained within Privacy Notices.
Privacy Notices	Notices given to Data Subjects, usually when they provide their Personal Data to NTU, which informs them about how the data will be used, whom it will be shared with, how long it will be held for, etc.
Regulatory Authority	Information Commissioners Office.

See NTU's [Data Protection Policy](#) for a fuller explanation of what is meant by "Personal Data" and "Special Category Data" and what "Processing" Personal Data means.

3. Regulatory Requirements

This Policy has been documented giving consideration to, and in compliance with the following regulatory requirements.

Regulatory Requirement	Status
Retained UK version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018 (UK GDPR)	UK Legislation
The Data Protection Act 2018	UK Legislation
Information Commissioner's Office (ICO)	UK Independent Body and data protection regulator / guidance
The Freedom of Information Act 2000 (FOIA)	UK Legislation

4. Responsibilities

4.1 University Executive Team (UET)

UET has overall responsibility to ensure NTU meets its legal and regulatory responsibilities under the UK GDPR, and to ensure compliance with this Policy.

4.2 Employees

It is the responsibility of managers to ensure that they provide sufficient and accurate data and that data are provided to Legal Services within the required timescales agreed.

It is the responsibility of all NTU employees to ensure that they have read and understood this Policy and to raise any concerns with non-compliance.

4.3 Legal Services and Data Protection Officer (DPO)

This Policy is owned by Legal Services,. Legal Services has the right to escalate any issues of non-compliance with this Policy to the DPO who may in turn escalate to UET should that be appropriate. The DPO can be contacted by emailing DPO@ntu.ac.uk.

5. Subject Access Requests (SAR)

5.1 Purpose

The UK GDPR clarifies the reasons for allowing individuals to access their Personal Data. This is to help individuals understand how and why an organisation is using their data, and check it is doing so lawfully.

9.1 Validity

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. There is no specific form of words or reference to legislation that makes a request valid, nor does it need to be directed to a specific contact within NTU. The data an individual has the right to obtain is as follows:

- Confirmation that their data is being processed;
- Access to/copies of their Personal Data; and
- Other supplementary information – this largely corresponds to information that should be provided in a privacy notice (see [Article 15](#) of the UK GDPR).

5.3 Verification

When a SAR is submitted, an individual must provide verification of their identity using 'reasonable means'. NTU must be satisfied of the identity of an individual to protect unauthorised access to Personal Data. If NTU does not have sufficient information to verify the identity of the individual and requests further proof of ID, the one-month time limit referred to in section 5.6 does not begin until the required ID has been received.

An individual can ask a third party (e.g. friend, solicitor, relative) to make a SAR on their behalf. In instances such as these, NTU must be satisfied that the third-party is entitled to act on the individual's behalf. It is the third party's responsibility to provide evidence of their authority.

5.4 Fees

SARs should be dealt with free of charge, unless the request is unusually large, complex, or an individual requests further copies of their data. If this is the case (the decision will be made by Legal Services) a reasonable fee may be charged. If a fee is charged, the one-month time limit does not begin until the fee is received.

5.5 Personal Data Released

NTU, as a Controller (through Legal Services) will supply all information available to them which an individual has requested and is entitled to receive under the legislation. Under the UK GDPR there are further stipulations in terms of what an individual can be entitled to receive. This is extracted below for reference:

1. *The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information (unless subject to an exemption – see Section 6 below):*
 - *the purposes of the processing;*
 - *the categories of personal data concerned;*
 - *the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
 - *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
 - *the 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;*
 - *the right to lodge a complaint with a supervisory authority;*
 - *where the personal data are not collected from the data subject, any available information as to their source;*
 - *the existence of automated decision-making, including profiling, referred to in [Article 22\(1\) and \(4\)](#) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*
2. *Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to [Article 46](#) relating to the transfer.*
3. *The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.*
4. *The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.*

5.6 Response Times / Seeking Clarification

Under the UK GDPR, NTU must comply with a SAR without undue delay and at the latest within one month of receiving the request. The time to respond to a SAR can be extended by up to a further two months if the request is unusually large or complex. Legal Services will make this decision and where it deems that this is the case, will explain to the individual, within the original one-month timeframe, its rationale for why there is a need for an extension and when they can reasonably expect to receive a response.

NTU are allowed to seek clarification from an individual, asking them to specify the information or processing activities their request relates to, if the remit of their request is not clear. This is especially helpful in circumstances where NTU processes a large amount of information about an individual. The time limit for responding to the request is paused until clarification is received.

5.7 Refusing a SAR

If a request is manifestly unfounded or excessive, particularly where it is repetitive, then the request can be refused.

Any decision to refuse a request will be made by Legal Services and should a request be refused, the Data Subject will be informed of the reasons why it is refused and of their right to complain to the Regulatory Authority, within one month of receipt of the request.

6. SAR Procedure

All SARs are dealt with **only** by the Legal Services Team.

To help the Legal Services Team facilitate a SAR as expeditiously as possible, it requests that all Data Subjects wishing to engage their right of access to follow this procedure:

- a) Where possible, make a request in writing, using the form [available on our website](#). This will come directly into Legal Services. You can contact us directly at DPO@ntu.ac.uk.
- b) The form will ask you to verify your identity. A copy of original documentation is acceptable. If sufficient ID to enable us to verify your identity is not submitted with the original request, we will request further information from you. Personal Data will not be released until verification of identification is confirmed; and
- c) The request should provide detail about the information you wish to request such as where and whom the information is believed to be held by. These details allow for efficient location and retrieval of the information requested. Should a request not be clear, or the scope too broad, NTU may need to seek clarification. The time limit for responding to a request is paused until clarification is received. Further information about preparing a SAR is available on the ICO website.
- d) Where a SAR is received within any area of NTU, other than Legal Services directly, the SAR must be forwarded to Legal Services within 2 working days of receipt of the SAR. Legal Services will acknowledge the SAR – the area where the SAR was received needs to take no further action on the SAR. This includes a request for personal data by third parties, such as solicitors.
- e) Where a SAR has been received, this will be assessed by Legal Services who may then request certain personal data (information contained within emails / documents etc) from specific areas across NTU. A timescale will be given to the school/Professional Services area for a response with the required information – usually this is within **3 working days** of the request for the information/Personal Data. All areas of NTU are expected to comply with a request for information/Personal Data from the Legal Services team and within the stipulated timescale required. any queries/questions can be directed to the Legal Services staff member who requested the information from you or the DPO (DPO@ntu.ac.uk).
- f) Legal Services will make the decision on what information is provided to the Data Subject and the information that falls within an exemption.

Data Subjects are only entitled to information which relates to them. A response may sometimes contain redactions (documents showing blanked-out text) or information may be removed entirely if an exemption under the Data Protection Act (DPA) 2018 applies. [Exemptions](#) protect particular types of information, or, for example, other Data Subjects or information about a third party to whom NTU owes a duty of confidence or privacy.

A Data Subject's right to see their personal data shall not adversely affect the rights and freedoms of other people.

Any queries about requests should be directed to the DPO at DPO@ntu.co.uk.

7. Minimum Standards

The minimum standards that Legal Services apply to SARs are demonstrated in the following table:

Policy Goal	Procedures	Accountable
SAR Policy is kept accurate and up to date	The DPO will ensure a plan is in place to review and update the SAR Policy.	DPO
Procedures are in place and communicated	SAR procedure is in place and regularly reviewed annually. The procedure is communicated and saved centrally, to ensure accessibility from all employees.	DPO
A designated team is in place for dealing with SARs	A designated team within Legal Services is in place to deal with SAR requests.	DPO
Internal Guidance	A dedicated data protection page/area is available and contains relevant policies and procedures .	DPO
External Guidance	Guidance on making a SAR a link to the online form on NTU's website .	DPO
All staff handling SARs have relevant training	All employees are provided with advice on how to recognise a SAR (online GDPR module). Designated Legal Services members receive training and guidance on handling SAR's.	DPO
Adequate ID is collected to verify an individual's identity	Legal Services Team assess request and will request ID/verification documents as appropriate for each SAR. Verification managed by Legal Services Team.	DPO
All SAR data should be sent securely	SAR responses are sent securely, via the ZendTo Portal.	DPO
Documentation	SAR requests maintained in the Legal Services system. Requests to be responded to within one month of receipt or extended as appropriate.	DPO

8. Records Management

Good records management is a benefit to NTU and not a burden. NTU has produced a [Retention Schedule](#) to ensure that it has a transparent and consistent position. The Schedule is managed by Legal Services and contains all the relevant official and corporate documentation produced by NTU. This will save storage space within the estate and provide a definitive guide as to how and where corporate information is stored.

It is expected that each School and Professional Services Department will have their own document management system (where appropriate), based on the NTU-wide retention schedule. There are risks which could arise as a result of inefficient/poor document management, such as:

- Inability to recover documents which leads to delays and a failure to meet deadlines;
- Making the assessment of a request more difficult;
- A risk of disclosure of records when they are inappropriate;
- Elevated costs of compliance; and
- Potential increase for complaints and repeated requests.