Governance and Legal Services

Subject Access Request (SAR) Policy

NOTTINGHAM TRENT UNIVERSITY | 50 Shakespeare Street, Nottingham, NG1 4FQ

NOTTINGHAM TRENT UNIVERSITY

Version Control

Document Reference:	GDPR003
Policy Owner:	Legal Services
Approval Committee:	University Executive Team (UET)
Version:	Version 1
Next Review Date:	May 2019

Policy History

Version:	Author:	Reason for Issue:	Date:
Version 1	Legal Services	New Policy	23 April 2018

Contents

1. Introduction

The General Data Protection Regulation (GDPR) gives you the right to find out about what 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 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.

2. Scope

This Policy 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.

3. Regulatory Requirements

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

Body	Regulation	Section / Paragraph
General Data Protection Regulation **(GDPR)**	Regulation	Articles 13 - 15
Information Commissioner's Office **(ICO)**	UK Independent Body/ Guidance	GDPR and SAR
The Freedom of Information Act **(FOI)** 2000	Regulation	All

4. Responsibilities

University Executive Team
The University Executive Team (UET) has overall responsibility to ensure NTU meets its legal and regulatory responsibilities under GDPR, and to ensure compliance with this Policy.

Employees
It is the responsibility of managers to ensure that they provide sufficient and accurate data, and to ensure the information provided is within the timescales agreed.

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

Legal Services
This Policy is owned and set by the Governance and Legal Services Team, which includes the DPO. The Governance and Legal Services Team has the right to escalate any issues of non-compliance with this Policy to UET.

5. Subject Access Request (SAR)

Purpose
The GDPR clarifies the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

Validity
A Subject Access Request (SAR) must be requested in writing to be a valid request, this can be done via methods such as letter or email. The data an individual has the right to obtain is as follows:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

Verification
When a SAR is submitted, an individual must provide verification of their identity using 'reasonable means', this will be required by NTU before any data is released to them.

Fees
SARs should be dealt with free of charge, unless the request is an unusually large or complex request, if this is the case a reasonable fee may be charged.

Data Released
As a Data Controller NTU will supply all information available to them, which an individual has requested and that individual is entitled to receive under the legislation. Under GDPR there are further stipulations in terms of what an individual can be entitled to receive:

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:*
   - *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.*

Response Times

Under the new GDPR regulation, SARs should be dealt with within one month of receipt, unless the request is an unusually large or complex request. If this is the case, communication should be made to the individual to explain the delay.

The minimum standards that NTU 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 annually review and update the SAR Policy.	DPO
Procedures are in place and communicated	SAR procedure is in place and 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 is in place to deal with SAR requests - this is within Legal Services.	DPO
Internal Guidance	A dedicated data protection page/area is set up with all relevant policies and procedures on SARs.	DPO
External Guidance	Guidance on making a SAR and a template form should be provided on the NTU website, the correspondence email to send it to, and the expected response time.	DPO
All staff handling SARs to have relevant training	All employees are trained as part of Data Protection, to recognise a SAR. Designated Legal Services members receive training and guidance on handling SAR's.	DPO
Adequate ID is collected to verify an individual's identity	A standard format email, requesting ID/verification documents is requested on every SAR. This must be received before any data is released.	DPO
All SAR data should be sent securely	All SAR data is to be sent securely, via the ZendTo Portal or via recorded and signed for delivery.	DPO
Documentation	A log will be kept of all SAR requests, with full details of the request and response times. Requests are to be dealt with and responded to within one month of receipt.	DPO

6. Guidance

If a SAR is received by anyone at NTU, you must contact the Legal Services Team DPO@ntu.ac.uk to notify them as soon as possible, this should include the request for Personal Data and any further information you may have/hold.

The designated team within Legal Services will deal with the request as per this Policy and the SAR Procedure.