Scope: Data Protection	Effective Date: May 2023	Responsible Dept: Governance & Compliance	Equality Analysis Undertaken:
Last updated by/date: May 2023	Next review date: May 2024	Associated links:	Policy ref:

Subject Access Request Policy

1. Introduction

The aim of this policy is to outline the process for receiving, processing, and responding to Subject Access Requests. The GDPR Right to Access allows individuals to request information about the way an organisation processes their data. Individuals are also given the right to request copies of their personal data in a readable and portable format. York St John University is required to comply with this aspect of the GDPR and demonstrate compliance to the Information Commissioner's Office (ICO).

2. Receiving a Subject Access Request

Subject Access Requests can be made in writing, electronically, or verbally. When a directorate or school receives a Subject Access Request, it should be immediately forwarded to the Governance and Compliance office via gov.compliance@yorksj.ac.uk. The Governance and Compliance team will provide the requester with a receipt, and will aim to process the request within one calendar month. If retrieval of the data requested is deemed to be complex, the University is permitted by the GDPR to extend the deadline by a further two calendar months (three calendar months from the date the request was initially received).

3. Verifying a Requester's Identity

3.1 It may be necessary to request proof of identification from the requester if the University is not satisfied that the requester is who they claim to be, or if the request has been made on behalf of someone else. The request for ID should be sent as soon as possible by the Governance and Compliance team, and the response time should be paused until the requester provides adequate proof of identification.

The requester should provide a copy of one of the following forms of identification:

- Birth Certificate
- Driving Licence
- Passport
- Proof of Age Card
- National Identity Card
- Medical Card
- Benefits letter

Original documents should not be accepted, and copies should be securely deleted as soon as the identity check is complete.

3.2 If a request is made on the behalf of the data subject (for example, by a solicitor or carer), the University should make every effort to ensure that the data subject is aware of the request and has given their consent for the data to be provided to the third party. The request made by the third party should not be forwarded to the data subject, and no personal details relating to the two individuals should be shared by the University with either.

4. Processing a Subject Access Request

4.1 A reasonable effort should be made to retrieve and, where requested, provide copies of the data requested. However, the University is not required to conduct searches that would be unreasonable or disproportionate to the importance of providing access to the information.

4.2 If the University genuinely requires further information in order to comply with the request, it is permitted to ask the requester to provide the relevant clarification. Until the further required information is received, the response time may be paused.

4.3 The University should consider the requirements of processing the request as soon as possible and retrieve the information in the most practical and efficient manner before mobilising the IT department. For example, it may be more reasonable to contact the most relevant departments/staff members and ask them to retrieve the data before running a more invasive network search.

4.4 Any employee who receives a request from the Governance and Compliance team for information to support the University's response must perform a thorough search of the records for which they are responsible. This may include, but is not limited to, emails (including archived emails and those which have been deleted but are still accessible), Word documents, spreadsheets, databases, systems, removable media, recordings, and paper records.

4.5 It may be necessary for the Governance and Compliance team to request that the IT department runs a remote search of the entire network, including mailboxes, to locate the relevant data. The IT department should perform the search as soon as possible and provide the Governance and Compliance team with full access to the search results in an accessible format.

4.6 The Governance and Compliance team are responsible for preparing the data for transfer to the requester. This may involve searching for and redacting information which is exempt from the request, such as third-party personal data and commercially sensitive data. Information about exemptions can be found below. Digital redactions should be made using a robust and reliable software solution such as Adobe Acrobat DC, and redactions must be factored into the permitted timescales.

5. Manifestly Unfounded, Excessive, and Repetitive Requests

Where requests are manifestly unfounded, excessive, or repetitive, the University may refuse to act on the request or charge a reasonable administration fee. The University must provide the requester with details of, and reasons for, its decision within one calendar month.

When considering whether the request is manifestly unfounded or excessive, the following circumstances should be addressed:

- the nature of the requested information;
- the context of the request, and the relationship between the University and the individual;
- whether a refusal to provide the information or even acknowledge if the University holds it may cause substantive damage to the individual;
- the University's available resources;
- whether the request largely repeats previous requests and a reasonable interval hasn't elapsed;
- whether it overlaps with other requests (although if it relates to a completely separate set of information, it is unlikely to be excessive);
- consider each request individually;
- do not presume that a request is manifestly unfounded or excessive just because an individual has previously submitted a manifestly unfounded or excessive request;
- the inclusion of the word "manifestly" means there must be an obvious or clear quality to unfoundedness/excessiveness; and
- ensure that the University has strong justifications for why it considers a request to be manifestly unfounded or excessive, which can be clearly demonstrated to the individual and the ICO.

6. Responding to a Subject Access Request

6.1 The University's response to the Subject Access Request should be approved by the Director of Governance, Assurance and Compliance and, where the request is more sensitive or may have a reputational impact on the University, the Data Protection Officer (DPO). It should then be submitted to the requester within one calendar month of the initial request (or up to three calendar months where the deadline has been extended). The response should be sent securely, which may require encryption, and should include details of how the requester can complain to the University and the ICO should they wish to.

6.2 Once the response has been sent, copies of the full request, including the relevant data, should be retained for one month by the Governance and Compliance team, and a record of the request retained for one year via the University's Subject Access Request Log.

7. Exemptions

There may be reasonable justification for applying an exemption when providing some or all of the requested data. A list of acceptable exemptions can be found at the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-other-exemptions-are-there/

8. Complaints

If the requestor is not satisfied with the response they've received, the University must manage this as a formal complaint. If the requester is unhappy with the outcome of the complaint, they may submit a complaint to the Information Commissioners Office. Details of how to make a complaint to the ICO can be found at: https://ico.org.uk/make-a-complaint/.