STOKE ON TRENT COLLEGE	**POLICY 53** **DATA SUBJECT ACCESS REQUESTS POLICY**	

1.0 Introduction

1.1 This policy defines the internal handling of data subject access requests received by Stoke on Trent College. The guidance provided in this policy should be used to ensure such requests are dealt with in a structured, transparent and fair manner.

1.2 The General Data Protection Regulation (GDPR)/DPA 2018 grants all individuals the right to access their person data held with any establishment and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing.

1.3 Definitions

"**Information asset"**	refers to a set of data in hardcopy/ manual or electronic format (e.g. paper records, databases, systems)
"**Data subject"**	means the person which the personal data relates to
"Personal data"	this is data which relates to a living individual who can be identified (a)from that data, or (b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
"Redaction"	means permanently and securely removing data that is exempt from disclosure from the material released to the requestor.

"**Sensitive personal data" (Special Categories)**	refers to trade union membership, sexuality, race or ethnicity, religious beliefs, political opinions, health and criminal records.
"**Employment records"**	this is information held by the controller which relates to a member of staff, present, past or prospective, whether permanent, temporary or a volunteer.
"GDPR"	The General Data Protection Regulation/DPA 2018 came into force in 2018. It harmonises data protection laws across the EU and updates the previous regulations to take full account of globalisation, and the everchanging technology landscape. Businesses will now need to demonstrate that they comply with the regulation when handling personal data. The regulation applies to any company processing the personal data of individuals in the EU in relation to offering goods and services, or else to monitor their behaviour. Significant penalties can be imposed on employers who breach the GDPR, it is therefore very important that businesses meet all the requirements, one of which is the processing of subject access requests.

2.0 What is a data subject access request?

2.1 A data subject access request is a request from an individual (the data subject), in which they ask to be provided with information regarding the personal data we process concerning them.

2.2 The GDPR requires that the information you provide to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. It also states that:

- You must provide the requested information free of charge

- You can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive
- You can charge a reasonable fee to comply with requests for further copies of the same information. The fee must be based on the administrative cost of providing the information.

3.0 Who can make a data subject access request?

3.1 The following people can submit a data subject access request:

- The individual themselves
- Individuals requesting access on behalf of a child for whom they have parental responsibility
- A representative nominated by the individual to act on their behalf, such as solicitors or a relative, where there is valid consent by the individual granting authority.

3.2 Data subject access requests can be made in any form, including via post, email, telephone and social media.

4.0 Proof of ID

4.1 In accordance with the GDPR/Data Protection Act 2018, you are not required to process the request until the identity of the requestor has been verified.

4.1.1 Individuals requesting their own personal data will need to provide the following:

- Photographic proof of identity (e.g. passport or full UK driving licence)
- Proof of address (e.g. a recent utility bill, bank statement)

4.1.2 Individuals requesting the personal data of another individual will need to provide then following:

- Signed consent from the data subject stating that the requestor has their permission to make the request on their behalf.

5.0 What information can they request?

5.1 Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them; however, subject access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed;
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Given a copy of the personal data; and
- Given details of the source of the data (where this is available)

5.2 An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

6.0 Exemptions, Refusals and Redactions

6.1 Some information is exempt from disclosure under the terms of the GDPR and, in some cases, you may not be able to explain to the requestor why you are unable to disclose the requested information. Detailed guidance is available from the Information Commissioner's Office website.

6.2 Where a request is manifestly unfounded, vexatious, repeated or excessive, Stoke on Trent College holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

6.3 If a large quantity of information is being processed about an individual, Stoke on Trent College will ask the individual to specify the information the request is in relation to.

6.4 Redactions may be required where there is some information concerning other data subjects contained in the documents and consent from those individuals cannot be achieved.

7.0 Scope and application

7.1 All employees are responsible for supporting the handling of data subject access requests made to Stoke on Trent College, as such requests may be received by any department or employee. It is therefore essential that this policy is adopted and supported by all.

STOKE ON TRENT COLLEGE	POLICY 53 **DATA SUBJECT ACCESS REQUESTS POLICY**	

Handling Data Subject Access Requests

8.0 Responsible department / person

8.1 The DPO Lead is responsible for the handling of data subject access requests made to Stoke on Trent College.

8.2 Once received, the DPO Lead will investigate and respond to the request accordingly, taking into account the requirements of the GDPR/DPA 2018.

9.0 Responsibilities of all other employees

9.1 The DPO Lead is solely responsible for responding to all data subject access requests received by Stoke on Trent College.

9.2 All other employees are prohibited from responding to any data subject access request and, for the purposes of this policy, are defined as "unauthorised employees".

9.3 If a data subject access request is received by an unauthorised employee, details of the request and any accompanying documents are to be forwarded to the DPO Lead via dpo@stokecoll.ac.uk.

9.4 It is essential that requests are forwarded on the day of receipt.

9.5 If any communication is received from the Information Commissioner's Office, the Supervisory Authority is to be informed immediately. Unauthorised persons are prohibited from responding to any such communications from the Supervisory Authority.

10.0 Timescales

10.1 The DPO Lead must comply with a subject access request without undue delay and in any event within **30 calendar days** of the date on which the request is received or, if later, the day on which the College received:

- Any requested clarification of what the information requested is; and
- Any information requested to confirm the requestors identify

10.2 If more time is needed to respond to complex requests, an extension of **another two months** is permissible. This should be communicated to the data subject in a timely manner within the first month.

10.3 If the DPO Lead cannot provide the information requested, the data subject should be informed of this decision without delay and at the latest within one month of receipt of the request.

11.0 Approval

Approved by the College Executive Team

Signed:

(Principal)

Endorsed by the College Corporation

Signed:

(Chair)