The Sheffield College

Data Protection Policy

Owner: Data Protection Officer	**Related Strategies:**
Relevant to: all processing undertaken by the College that involves personal data as defined in section 2	

Office Use only:

Corporate Intranet Family:	Approval Board/Committee/Group: ARAC Executive Owner: EDSSI	Approval/Re-approval Date: 06 July 2022	Implementation Date: 25 May 2018	Next Review Date: July 2023

The Sheffield College

New Policy or Substantive Policy Review

Version	Date	Policy Development Agreed by *(Executive Owner)*	Policy Development Author	Draft Policy Verified by	Policy Approval	Impact Assessment *(if applicable)*
1	2018	**ELT**	**DPO**	**ARAC**	**Governing Body**	

Rationale for new or substantive policy review	Changes to laws and regulations

Please make explicit if change/review relates to procedures, guidelines and associated documents only

Periodic Policy Review / Change History

Version	Date of Review / Revision	Description of Change	Reviewed By	Approved By *(Executive Owner)*
2	July 2022	• Replacement of descriptive sections 1 Overview and 2 About this Policy with a more succinct Policy Statement (and renumbering throughout) • Section 2 Definitions, minor updates to defined terms • Addition of new Section 3 Principles previously in Section 5 Data Protection Principles • Addition of new Section 4, Scope and Limitations, in line with college policy template • Replacement of previous section 4 (College Personnel's General Obligations) with new section 4 Responsibilities covering Governors, managers and staff • Addition of new Section 6 Operational Controls, summarising and replacing previous sections 6, 7, 8, 9 and 10 • New Section 7 (replacing old S.11) on reporting a data breach • New Section 8 on responding to governmental and law enforcement requests so staff can easily find this • Transferring old sections that described the GDPR into relevant procedures implementing the protections. S.12 (appointing contractors), s.13 Individual rights, s.14 Marketing and consent, s.15 Automated decision making, s.16 Data Protection	ARAC	EDSSI

		Impact Assessments; s.17 Transferring personal data outside EEA		

Communication

To be agreed by Executive Leadership Team

Announcement on hub ✓	SLT email □
College newsletter □	All staff email ✓
SLT meeting □	Cascade brief □
External website ✓	Training needed (all staff) ✓

1. POLICY STATEMENT

The Sheffield College ("College") collects and processes Personal Data in order to carry out its functions and provide services to College Personnel and students.

This policy sets out how the College's handling and processing of Personal Data is done in an effective, accountable and transparent fashion to ensure compliance with the requirements of Data Protection Laws.

The College is committed to ensuring all processing activities are carried out in accordance with all applicable Data Protection Laws and regulations. This policy sets out what is expected of College Personnel and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data controlled or processed by the College.

Compliance with this policy is crucial to maintaining confidence of the Data Subjects and third parties whose Personal Data is processed by the College. All College Personnel and third parties must comply with the policy and any breach of this policy will be taken seriously and may result in disciplinary action.

In line with the requirements of data protection legislation the College is registered with the UK Information Commissioner's Office with registration number: Z667180X.

2. DEFINITIONS

College – The Sheffield College, Sparks Managed Services, Sparks Teaching Services and Sparks Solutions Ltd which are wholly owned subsidiary companies within the Sheffield College Group
College Personnel – Any College or College Group employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.
Data Controller – Any entity (e.g., company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.
Data Processor – Any entity that processes data on behalf of a Data Controller
Data Protection Laws – The UK GDPR and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.
Data Protection Officer – The Data Protection Officer is appointed by the Chief Executive Officer and Principal to carry out the statutory and other duties for oversight of this Policy and related procedures. Our Data Protection Officer is Seb Smith, and can be contacted at: DPO@sheffcol.ac.uk
Data Subject – Living individuals who can be identified, directly or indirectly, from information that the College has.

EEA – includes EU countries, Iceland, Liechtenstein and Norway. The United Kingdom (UK) ceased to be a Contracting Party to the EEA Agreement after its withdrawal from the EU on 31 January 2020.
ICO – the Information Commissioner's Office, the UK's data protection regulator.
Personal Data – Any information about a Data Subject which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.
Special Category Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health, sexual life or sexual orientation and criminal records. Special Categories of Personal Data are subject to additional controls.
UK GDPR – The retained EU law version of the General Data Protection Regulation ((EU) 2016/679)

3. PRINCIPLES

There are seven key principles of Data Protection as defined in both the UK GDPR and the Data Protection Act 2018. These require that Personal Data is:

processed lawfully, fairly and in a transparent manner: any processing of Personal Data must be known to the Data Subject (transparency), must match the description given to the Data Subject (fairness), and for a purpose permitted under data protection regulations (lawfulness).

collected only for specified, explicit and legitimate purposes: The College or the third-party Data Controller must specify what the Personal Data will be used for and limit the processing of that Personal Data to only what is necessary to meet the specified purpose (purpose limitation).

adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed: The College must not store any Personal Data beyond what is strictly required (data minimisation).

accurate and where necessary kept up to date: The College must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data (accuracy).

stored for no longer than is necessary for the purposes for which it is processed and in a way that limits or prevents identification of the Data Subject (storage limitation).

processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (security, integrity and confidentiality).

stored and processed in an accountable manner: The College and/or the third-party Data Controller shall be responsible for and be able to demonstrate compliance with the data protection principles.

4. SCOPE AND LIMITATIONS

This document defines the data protection policy for all activities of the College. It applies to all Personal Data as defined by the UK GDPR which is processed by the College and College Personnel.

The College has the role of Data Controller in relation to the Personal Data it holds in respect of College Personnel and students.

For further UK GDPR references visit the ICOs website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

5. RESPONSIBILITIES

The Governing Body is responsible for approving the policy framework and monitoring that it is effective in achieving compliance with the laws.

The Chief Executive Officer and Principal and College Executive Team have overall accountability for data protection within The College and are responsible for ensuring that the Policy is implemented through the organisation.

The College have appointed an independent Data Protection Officer (DPO) responsible for advising the CEO and the Executive Team on the College's compliance with Data Protection Laws. The Head of IT and Development has responsibility for implementation of the technology platform and information security within the College to support compliance with Data Protection Laws.

The DPO is responsible for overall governance of and providing guidance to the College's operations relating to Personal Data and for monitoring compliance with Data Protection Laws and this policy.

College Personnel must be familiar with this policy, data protection requirements and the appropriate associated procedures. Each department works with the DPO to maintain records of their Personal Data processing operations.

College Personnel must act in accordance with the procedures outlined the appropriate documentation (including responding to Subject Access Requests (SARs) and performing Data Protection Impact Assessments (DPIAs)).

6. OPERATIONAL CONTROLS

The College will ensure operational compliance with applicable Data Protection Laws and this policy through appropriate management, application of documented procedures, risk criteria and controls including the following:

Data Protection Training

All College Personnel understand that they are responsible for following good data protection practice, is appropriately trained to do so and is appropriately supervised.

Records of Processing
Each department work with the DPO to maintain records of their Personal Data processing, describing what Personal Data is held and its methods of handling/processing Personal Data and undertakes impact and risk assessments on its Personal Data processing.

Data Protection by Design & Data Protection Impact Assessments
Data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes.

Each department must ensure that a Data Protection Impact Assessment is conducted for all new and/or revised processes that are likely to result in a high risk to individuals for which they have responsibility for processing Personal Data.

Privacy Notices
The College makes available a privacy notice for Data Subjects which informs them of how their data is processed, fulfilling the requirements of applicable law.

Subject Access Rights & Requests
Queries about handling Personal Data are promptly and courteously dealt with and the College ensures that the rights of people about whom information is held, can be fully exercised in accordance with applicable law.

Under UK GDPR rights include: the right to be informed that processing is being undertaken, right of access to your own Personal Data, right to prevent processing in certain circumstances and the right to correct, rectify, block or erase data which is incorrect.

Data Transfers
The College may transfer Personal Data to internal or third-party recipients in order to fulfil the purpose for which Personal Data is held. Where necessary, the College ensures that agreements are in place with such third parties to provide appropriate safeguards and legal protection for the rights of the relevant Data Subjects.

Compliance Monitoring
To confirm an adequate level of compliance is being achieved by all departments in relation to this policy, the DPO carries out regular data protection audits that will assess: compliance and awareness, information governance, systems and record retention, security of Personal Data and physical working locations.

7. PERSONAL DATA BREACH REPORTING

Any individual who suspects that a Personal Data breach has occurred leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data that is transmitted, stored or otherwise processed must immediately notify the DPO providing a description of what occurred.

The DPO will investigate all reported incidents to confirm whether a Personal Data breach has occurred. If a Personal Data breach is confirmed, the DPO will follow the relevant procedure based on the criticality and quantity of the Personal Data involved in accordance with the ICOs requirements.

For severe Personal Data breaches, the College's Executive Team will work with the DPO to initiate and chair an emergency response team to coordinate and manage the Personal Data breach response.

8. GOVERNMENTAL & LAW ENFORCEMENT REQUESTS

The College understands its responsibilities when assisting with enquiries from law enforcement agencies or public authorities.

Each request for information will be assessed on a case-by-case basis and clarification sought, where needed, from the requesting body. In particular, the College will ensure that the requester provide:

- Specifics of the request (i.e., the data they are seeking to access)
- The context of the request
- The reason why this data will assist in their enquiry/investigation

Any requests of this nature should be directed to the DPO. The College retain a log of all requests of this nature.

9. MONITORING AND REVIEW

The Policy will be reviewed annually or when Data Protection Laws require it.