SARACENS
MULTI-ACADEMY
TRUST

DATA SECURITY POLICY

Responsibility of *(see policy tracking sheet):*	Trust Board
Approved by:	Trust Board
Date Approved *(by above):*	September 2024
Next Review due by:	September 2026

Contents

1. Introduction ……. 2

2. Implementation of this Policy …… 2

3. Training …… 2

4. Data Security Standards …… 2

5. Filtering and Monitoring Standards ……. 3

6. Compliance with this Policy ……. 3

7. Review and Monitoring Arrangements …… 3

8. Links with Other Policies ……. 3

1. Introduction

Data security is the practice of protecting information from unauthorised access, corruption, theft, disclosure, destruction or modification/alteration throughout its entire lifecycle.

Saracens Multi-Academy Trust (SMAT) is committed to raising the awareness of data security within its schools. It achieves this through the application of appropriate policies and procedures, training and maintaining up to date hardware and software. The aim is to protect the security of data and avoid:

- Damage to reputation
- Financial loss
- Loss of confidentiality
- Physical damage to natural persons
- Any other significant economic or social disadvantage
- Loss, misuse or damage of IT and infrastructure
- Lack of awareness of staff in relation to their personal responsibility for managing data securely.

2. Implementation of this Policy

Responsibility for implementing and ensuring compliance with this policy lies with the Data Protection Team (DPT), which comprises, the Data Protection Officer (DPO), the Deputy Data Protection Officer (DDPO) and the Head of IT.

Data security and management is a responsibility of the SMAT and the DPT report directly to the Trust Board on data security matters.

3. Training

All staff, trustees, governors and volunteers with access to the Trust IT systems are required to complete mandatory induction training on data security and sign the SMAT ICT Acceptable Use Agreement before they are given access to Trust IT equipment or systems. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the schools' or Trust's processes make it necessary.

Pupils at Trust secondary schools are required to sign a Pupil ICT Acceptable Use Agreement before accessing the Trust's IT systems. All pupils in the Trust's schools will receive regular, age appropriate training on the safe use of the internet and data security.

4. Data Security Standards

The Trust, where possible, will comply with current DfE Cyber Security Standards for schools and colleges as updated from time to time. The document can be found here: Cyber security standards for schools and colleges.

The Trust will also comply with current Data Protection in Schools Guidance as updated from time to time. The document can be found here: DfE Data protection in schools.

5. Filtering and Monitoring Standards

The Trust, where possible, will comply with current DfE Filtering and Monitoring Standards for schools and colleges as updated from time to time. The document can be found here: Filtering and monitoring standards for schools and colleges.

6. Compliance with this Policy

All staff, trustees, governors and volunteers are required to comply with this policy.

Staff have an obligation to report potential and actual data protection failures or suspected failures to the DDPO (who is the Trust's Chief Financial and Operating Officer). The DPT will investigate as appropriate. Breaches involving special category data and other sensitive information will be reported to the DPO dpo@sapphireskies.co.uk .The DPO will decide whether any breach should be reported to the Information Commissioner's Office (ICO) and will liaise with the DDPO who will make any such report.

Where a member of staff has reason to believe that such a report has not been actioned, they may make a disclosure under the SMAT Confidential Reporting (Whistleblowing) Code.

7. Review and Monitoring Arrangements

The DPO working with the DDPO is responsible for monitoring and reviewing this policy. Changes are approved by the Trust Board.

8. Links with Other Policies

This Data Security Policy is linked to the:

- Child Protection and Safeguarding Policy
- Confidential Reporting (Whistleblowing) Code
- Data Protection Policy
- Data Retention Policy
- Freedom of Information Policy & Publication Scheme.