Sutton School and Specialist College Policy

For

Data Protection Policy

Date of first issue:	16th March 2018
Dates of Updates:	
Most recently approved by governors on:	28 March 2018
To be next reviewed on:	

Table of Contents

1. INTRODUCTION

1.1 Background

Sutton School & Specialist College is a purpose built day school for pupils aged 11-16 whose educational needs cannot adequately be met in mainstream schools. It creates and maintains an extensive range of innovative educational solutions and services - all designed or selected to meet the specific needs of its students.

Pupils are taught in an atmosphere of positive recognition where each person's individuality and talents receive encouragement and nurture. School strives to work in partnership with parents. There are parent's evenings throughout each year together with an annual review of each child's educational program through the review of the statement/EHCP.

Everyone in the school strives to work together in a community of mutual respect regardless of race, class, colour or creed. All students are consulted about their education through weekly mentor groups/ tutor time.

We endeavour to bring out the best in our pupils so that they mature into adults capable of an independent life which will be personally rewarding and of service and benefit to their local communities.

1.2 Purpose and scope of this Policy

The Data Protection Policy is designed to provide an overview of how data protection is managed at Sutton School & Specialist College.

It sets out the following:

- Data protection policy and objectives
- The data protection framework
- Legal compliance, e.g. with the GDPR

This Policy is intended for circulation to Sutton School & Specialist College staff, parents and other interested parties. It is supported by an internal data protection framework that provides staff with detailed guidance on how to ensure that this policy is effectively implemented.

2. POLICY, OBJECTIVES AND SCOPE

2.1 Data Protection Policy Statement

The Data Protection Policy of Sutton School & Specialist College recognises, observes and protects the rights of data subjects in regard to any of their personal data that the school collects, processes and stores, in accordance with all applicable legal, regulatory and contractual obligations.

This Policy has been approved by the School Governing Body on behalf of Dudley MBC. The Policy will be reviewed annually.

2.2 Objectives

The objectives of the Data Protection Policy are to:

- Communicate Sutton School & Specialist College Data Protection commitment to employees, parents/carers and other third parties;
- Summarise how the school's approach to data protection management is designed to be compliant with data protection legislation;
- Summarise governance arrangements for data protection management.

2.3 Scope

The scope of the Data Protection Policy covers:

- All personal data collected and / or processed by the school in the conduct of its business, in any format;
- All services developed and provided by Sutton School & Specialist College
- All Sutton School & Specialist College staff.

3. DATA PROTECTION FRAMEWORK

3.1 Sutton School & Specialist College as Data Controller

Sutton School & Specialist College acts as a data controller for the following categories of data subjects:

- Employees
- Former employees
- Students
- Parents
- Governors
- Professionals & Consultants
- Other service related suppliers

3.2 Sutton School & Specialist College as Data Processor

Sutton School & Specialist College, and its associated provisions, acts as a data processor with regard to the processing of personal data for the following categories of data subjects:

- Persons who work or volunteer for Sutton School & Specialist College
- Students & Parents: where Sutton School & Specialist College processes their data in order to provide services to the data controller (educational establishment customer)
- Examination candidates
- Clients:
    - Individual consumer clients
    - Education Establishment clients who require Sutton School & Specialist College to process personal data in order to deliver services
- Suppliers
    - Consultants
    - Staff working for organisations
- Third parties

Sutton School & Specialist College enacts its obligations as a data processor with regard to:

- Legal requirements
- Contracts
- Terms & Conditions
- Privacy Policy

3.3 Provision of Services

Sutton School & Specialist College delivers services to stakeholders in accordance with:

- Legal, regulatory and contractual requirements
- Sutton School & Specialist College's Privacy Policy

3.4 Consent

Sutton School & Specialist College reflects legal requirements relating to consent in the following ways:

- How consent is obtained, recorded and managed in its systems
- Data retention and deletion procedures
- Marketing procedures, including taking photos of data subjects
- Terms & Conditions
- Privacy Policy

3.5 Individuals' Rights

In accordance with data protection legislation, Sutton School & Specialist College recognises that data subjects have specific rights that must be protected and observed.

3.5.1 Right to be informed

Sutton School & Specialist College provides employees, parents and other third parties with information about how personal data is collected, processed and managed. It seeks to provide this information in language that is clear, concise and intelligible. This information is intended to be easily accessible for internal and external users.

3.5.2 Right of access

Sutton School & Specialist College provides data subjects with access to the personal data that it manages as a data controller. A Subject Access Request (SAR) process has been defined (see 3.7 below) and communicated. Data subjects for whom Sutton School & Specialist College is not the data controller but may process their personal data, should contact the data controller directly when requesting such access.

3.5.3 Right to rectification

Sutton School & Specialist College recognises the right of individuals to have inaccurate or incomplete data to be amended. Sutton School & Specialist College employees should initially make a rectification request to HR. Data subjects for whom Sutton School & Specialist College is not the data controller, should – in the first instance – contact the data controller when making a data rectification request. Queries or complaints should be made to the Data Protection Officer (dcharles@sutton.dudley.sch.uk)

3.5.4 Right to erasure

Sutton School & Specialist College recognises the right of individuals to request for their data to be deleted or removed where there is no compelling reason for its continued processing.

Sutton School & Specialist College will, in all cases, follow the ICO's guidance on how and when such a request should be observed.

Sutton School & Specialist College maintains a data retention schedule so that personal data is not retained for longer than is necessary with regard to the purpose for which the data was original collected. This may include logging data that is temporarily retained for diagnostic purposes. However, some personal data may be required to be retained in order to observe other legal or regulatory obligations. In addition, in line with the ICO's guidance on the constraints that exist when deleting data retained in digital back-ups, Sutton School & Specialist College will seek to place such back-ups beyond effective use.

3.5.5 Right to data portability

Where the right of portability applies, as defined by the ICO, Sutton School & Specialist College will provide data in a form that is structured, commonly used and in a machine readable form. In most cases, this will be the CSV format.

3.5.6 Right to object

Sutton School & Specialist College recognises the right of individuals to object to the processing of their personal data, where such objections are allowable under data protection legislation. This right is recognised in Sutton School & Specialist College's Privacy Policy.

3.5.7 Rights related to automated decision making including profiling

Sutton School & Specialist College does not use automated decision making where such decisions have a significant effect on data subjects.

3.6 Data Retention

Sutton School & Specialist College has established a data retention framework for employee and former employee data. The framework is based on statutory and non-statutory guidance, and is also aligned with guidance from HR professional organisations. The framework applies to both digital and non-digital data.

In regard to the retention of personal data of individuals who are neither employees nor former employees, data retention schedules will be applied in accordance with the following:

- Contracts
- Product-specific and service-specific data retention schedules

Data retention schedules will be documented and will be communicated, either through Terms & Conditions, or upon request.

3.7 Subject Access Requests

Sutton School & Specialist College has an established Subject Access Request (SAR) process for personal data for which it is the data controller.

Documented procedures are closely aligned to published guidance from the ICO and will be updated in line with any changes published by the ICO.

3.8 Data Security

Sutton School & Specialist College regards data security as a critical component of data protection compliance.

Data security controls include but are not limited to:

- Physical security controls
- Access management
- Asset management
- Encryption of data and devices
- Secure communications
- Anti-malware and anti-virus protection
- Firewalls and network monitoring
- Secure disposal of equipment
- Data Security training for employees

A programme of internal and external audits is used to monitor compliance and identify areas of potential improvement.

3.9 Data Breaches

All security incidents are logged on an internal security incident management system. They are reviewed and evaluated by a member of the security management team.

A security incident that involves personal data will initially be categorised as a Potential Data Protection Incident. If it is determined that a data breach has indeed occurred, this will trigger a formal Data Breach procedure.

If a data breach relates to employee data, Sutton School & Specialist College will inform the ICO in accordance with the ICO's published guidance.

If the data breach relates to student, parent or third party data, Sutton School & Specialist College will notify the relevant data controller.

3.10 Use of CCTV

Sutton School & Specialist College operates CCTV on the premises. The operation of CCTV is governed by the CCTV Policy, which is closely aligned with the ICO's guidance on this subject.

A copy of this policy is available upon request.

3.11 Transfer of personal data to a country outside the EEA

Sutton School & Specialist College does not transfer personal data outside of the European Economic Area. Detailed information on data transfer is outlined in the privacy policy as well as standard Terms & Conditions for relevant services.

3.12 Roles and Responsibilities

The following roles / functions relate directly to data protection management in Sutton School & Specialist College.

3.12.1 Data Protection Officer

Sutton School & Specialist College is required to appoint a Data Protection Officer (DPO) due to the following requirement of the GDPR:

- A DPO must be appointed where the core activities of the organisation involves the processing of large volumes of "special categories of personal data".

The DPO carries out the following functions in relation to data protection:

- Ensuring that data protection policy and practice meets legal, regulatory and statutory requirements
- Reporting to the highest level of management on data protection compliance
- Acts as a point of contact for data subjects, stakeholders, Sutton School & Specialist College management and regulatory authorities in regard to data protection matters

The DPO can be contacted at dcharles@sutton.dudley.sch.uk

3.12.2 Legal Services

Sutton School & Specialist College legal services carries out the following functions in relation to data protection:

- Ensuring that data protection policy and practice meets legal, regulatory and statutory requirements
- Ensuring that the Terms & Conditions for all products and services are legally compliant
- Ensuring that the Privacy and Cookies Policies are legally compliant
- Providing legal advice on data protection compliance

3.12.3 HR Services

Sutton School & Specialist College's HR department carries out the following functions in relation to data protection:

- Ensuring that personal data relating to employees, former employees, students, parents/ carers and third parties are processed in accordance with legal, regulatory and statutory requirements
- Maintaining a data retention schedule for digital and non-digital records
- Incorporating appropriate references and requirements to data protection in employee contracts and induction programmes

3.12.4 Employees

Contracts for Sutton School & Specialist College employees set out a number of obligations relation to information security, including data protection.

In addition employees are required to abide by a number of policies that relate to data protection:

- Acceptable Usage Policy & Security Guidelines
- Data Classification and Handling Policy

3.13 Governance

Sutton School & Specialist College has established a governance framework for data protection:

3.13.1 Data Protection Governors

The Governors are accountable for Sutton School & Specialist College's compliance with all relevant legal and regulatory obligations and frameworks. It therefore holds the Headteacher to account in regard to data protection compliance.

The Board of Governors ensure that relevant risks are identified, assessed and, where appropriate, further mitigated. Internal and external audits support this process.

3.13.2 Data Protection Officer (DPO)

The Headteacher is responsible for data protection management. The DPO approves policy and sets data protection priorities. They receive and evaluate regular reports from the Data Protection Officer, on behalf of the Board. It receives and evaluates an annual Data Protection Report, based on an assessment from an independent security consultant.

3.13.3 GDPRC (General Data Protection Regulation Committee)

The GDPRC is responsible for the implementation of information security and data protection policy and procedures across the Group. It approves and monitors an annual programme of security and data protection projects and initiatives. It sets and monitors a minimum standard of security practice across the school.

The Headteacher, Deputy Headteacher, Business Manager, Safeguarding Officer and the ICT Manager, sit on the GDPRC.

3.14 Training and Awareness

Sutton School & Specialist College provides information security and data protection training to all employees upon induction, which is refreshed annually. In addition, a number of communications initiatives are run in order to maintain or increase employees' awareness of data protection.

3.15 Assurance

Sutton School & Specialist College and its IT service provider RM carries out a range of assurance activities to help ensure that the organisation adheres to its security and data protection policies and procedures.

Such activities include:

- Internal/ external audits
- Security testing by independent third parties
- Data protection compliance review by independent third parties

4. LEGAL COMPLIANCE

4.1 Applicable Legislation

The following legislation is relevant to data protection legal compliance:

- Data Protection Act 1998
- General Data Protection Regulation (GDPR) (to be enshrined in UK law in 2018)
- Privacy and Electronic Communications Regulations (PECR) 2015
- Investigatory Powers Act 2016
- Protection of Freedoms Act 2012

4.2 Legal Basis for Processing Data

The legal basis for Sutton School & Specialist College processing personal data varies according to the nature of the activity being undertaken:

- Consent of the data subject
- Necessary for the performance of a contract, e.g. storing of employee and student data
- Processing for compliance with a legal obligation, e.g. retention of some employee data
- For the purposes of legitimate interests
- Legal obligation

4.3 Regulatory authority

The regulatory authority for Sutton School & Specialist College is the Information Commissioner's Office (ICO).

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113
Email: https://ico.org.uk/global/contact-us/email/

4.4 ICO Registrations

Sutton School & Specialist College has the following registrations:

Organisation name: **SUTTON SCHOOL**
Registration reference: **Z577947X**

Further details about these registrations are available from the ICO here.

5. APPENDIX A: DEFINITIONS

5.1 Personal Data

Sutton School & Specialist College uses the following definition of personal data.

> *"Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to **an identifier** such as a name, an identification number, **location data**, online identifier or to one or more factors specific to the physical, physiological, **genetic**, mental, economic, cultural or social identity of that person.*

GDPR, Rec.26; Art.4(1)

5.2 Special Categories of Personal Data

Sutton School & Specialist College uses the following definition for sensitive or "special categories" of personal data.

> *"Sensitive Personal Data" are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; **genetic data or biometric data**. Data relating to criminal offences and convictions are addressed separately (as criminal law lies outside the EU's legislative competence).*

GDPR, Rec.10, 34, 35, 51; Art.9(1)

5.3 Data Controller

Sutton School & Specialist College uses the following definition for the term "data controller":

- *"A controller determines the purposes and means of processing personal data."* (ICO)
- *"Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws.*

GDPR, Art.2(d)

5.4 Data Processor

Sutton School & Specialist College uses the following definition for the term "data processor":

- *"A processor is responsible for processing personal data on behalf of a controller."* (ICO)
- *"Processor" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."*

GDPR, Art.2(e)

6. DOCUMENT INFORMATION

6.1 Version History

Version	Status	Comment	Date
0.1	Draft	1st draft for GDPRC and stakeholder review.	15.03.18
1.0	Definitive	Authorised by GDPRC	28.03.18

6.2 Related Documents

Document	Date
Data Protection Act	1998
General Data Protection Regulation	2016

6.3 Change Management

This document will be changed as a result of review.