Sydenham School
Data Protection Policy

Approved by:	Full Governing Body	**Date:** June 2026
Last reviewed on:	June 2026	
Next review due by:	June 2027	

Contents

Contents 2
1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The Data Controller 4
5. Roles and Responsibilities 4
6. Data protection principles 5
7. Collecting personal data 6
8. Sharing personal data 7
9. Subject access requests and other rights of individuals 8
10. Parental requests to see the educational record 10
11. Biometric recognition systems 11
12. CCTV 11
13. Photographs and videos 11
14. Artificial intelligence (AI) 12
15. Data protection by design and default 12
16. Data security and storage of records 13
17. Disposal of records 13
18. Personal data breaches 14
19. Complaints 14
20. Training 14
21. Monitoring arrangements 14
22. Links with other policies 14
Appendix 1: Data Breach Procedure & Reporting Template 16

1. Aims

Sydenham School aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, volunteers, visitors, and other individuals is collected, stored and processed in accordance with UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and other regulations ("together Data Protection Legislation").

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Legislation.

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR, Data Protection Act 2018, the Data (Use and Access) Act 2025, which complements the afore mentioned UK's Data protection laws, the ICO's Code of Practice for Subject Access Requests and the Department for Education (DfE) position on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Data	Any information which is stored electronically, cloud-based, on a computer, or in certain paper-based filing systems.
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: › Name (including initials) › Identification number › Location data › Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: › Racial or ethnic origin › Political opinions › Religious or philosophical beliefs › Trade union membership › Genetics › Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes. › Health – physical or mental › Sex life or sexual orientation

TERM	DEFINITION
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data. They are responsible for establishing practices and policies in line with Data Protection Legislation.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Workforce	Includes any individual employed at/by the school, such as staff and those who volunteer in any capacity for the school, i.e., the school's governors.

4. The Data Controller

Sydenham School processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a Data Controller with the ICO and renews this registration on an annual basis or as otherwise legally required.

5. Roles and Responsibilities

This policy applies to **all members of staff** employed by Sydenham School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action and volunteers may be removed.

5.1 Governing Board

The Governing Board has overall responsibility for ensuring that Sydenham School complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

Sydenham interims School's DPO is:

Ms Simone McAllister, School Business Manager, Sydenham School, Dartmouth Road, London, SE26 4RD, s.mcallister@sydenham.lewisham.sch.uk , Tel. 020 8699 6731.

She will:

- Undertake his tasks independently – report to Head Teacher directly.
- Be point of contact for public for data protection issues.
- Be involved in timely manner in all data protection issues.

- Inform and advise the school, processors, and employees of obligations.
- Monitor data protection compliance.
- Advise as required on Data Protection Impact Assessments.
- To co-operate with supervisory authority, Information Commissioner's Authority (ICO).
- To act as contact point for the supervisory authority (ICO).
- Have due regard to the risk associated with processing, taking account of nature, scope, and context of processing.

5.3 The Data Controller

The Data Controller manages and oversees data handling and data protection by the school on a day-to-day basis. He is also responsible for maintaining the notification of registration for Sydenham School with the Information Commissioner's Office on an annual basis.

Sydenham School's Data Controller is Mr Martin Brooks, Director of Data, Assessment and IT Services – m.brooks@sydenham.lewisham.sch.uk , Tel. 020 8699 6731.

5.4 Headteacher and School Business Manager

The Headteacher and the School Business Manager act as the representatives of the Data Controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the school of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The UK GDPR is based on data protection principles that Sydenham School must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner and in line with the data subject's rights.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.

- Processed in a way that ensures it is appropriately secure.
- Must not be transferred to people or organisations situated outside the UK without adequate protection and assurances in place.

This policy sets out how the school aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. For personal data to be processed fairly, data subjects must be made aware:

- That the personal data is being processed.
- Why the personal data is being processed.
- What the lawful basis is for that processing (see below).
- Whether the personal data will be shared, and if so with whom.
- The period for which the personal data will be held.
- The existence of the data subject's rights in relation to the processing of that personal data; and
- The right of the data subject to raise a complaint with the Information Commissioner's Office in relation to any processing.

We will only obtain such personal data as is necessary and relevant to the purpose for which it was gathered and will ensure that we have a lawful basis for any processing. For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation.

We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract, i.e., an employment contract.
- The data needs to be processed so that the school can **comply with a legal obligation**.
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest, and carry out its official functions and duties.**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- Where none of the above apply then we will seek and rely on the individual's (or their parent/carer when appropriate in the case of a pupil) freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent.**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- The data has already been made **manifestly public** by the individual.
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights.**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

This will be done in accordance with the school's record retention schedule/records management policy.

8. Sharing personal data

8.1 Notifying data subjects

If we collect personal data directly from data subjects, we will inform them about:

- Our identity and contact details as Data Controller and those of the DPO.
- The purpose or purposes and legal basis for which we intend to process that personal data.

- The types of third parties, if any, with which we will share or to which we will disclose that personal data.
- If personal data will be transferred outside the UK, what safeguards are in place.
- The period for which their personal data will be stored, by reference to our Retention and Destruction Policy.
- The existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and
- The rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

Unless we have already informed data subjects that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive personal data about a data subject from other sources, we will provide the data subject with the above information as soon as possible, thereafter, informing them of where the personal data was obtained from.

8.2 Sharing Personal Data with others

Our Privacy Notices set out what data processing we undertake. We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we will seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

We will process all personal data in line with data subjects' rights.

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed.
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned.
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- Where relevant, the existence of the right to request rectification, erasure, or restriction, or to object to such processing.
- The right to lodge a complaint with the ICO or another supervisory authority.
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request in any form, they must immediately forward it to the School Business Manager.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at Sydenham School may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification.
- May contact the individual via phone to confirm the request was made.
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge.

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent, and it would be unreasonable to proceed without it.
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

As a maintained school where a parent is only seeking copies of the child's educational record, consent will not be sought from the child and this request will be responded to as set out in Section 10 below as parents can access the education record in their own right.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing that has been justified on the basis of public interest, official authority, or legitimate interests.
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils, for example, pupils can pay for school dinners cashless with a provided PIN.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Facilities Manager or the Premises Team.

However, CCTV footage should only be reviewed for the following reasons:

- Make members of the school community feel safe.
- Protect members of the school community from harm to themselves or to their property.
- Deter criminality in the school.
- Protect school assets and buildings.
- Assist police to deter and detect crime.
- Determine the cause of accidents.
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings.
- To assist in the defense of any litigation proceedings.

The CCTV system should not be used to:

- Encroach on an individual's right to privacy.
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring.
- Pursue any other purposes than the ones stated above.

In any case, members of our staff can request to look at CCTV footage relating to a dispute, but the authorisation for this lies with the Headteacher, her Deputies or the DSL.

13. Photographs and videos

As part of Sydenham School activities, we may take photographs and record images of individuals within Sydenham School.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on Sydenham School website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Please see our Safeguarding Policy for more information on our use of photographs and videos.

14. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Sydenham School recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Sydenham School will treat this as a data breach and will follow the personal data breach procedure outlined in appendix 1.

15. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply.

- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of Sydenham School and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

16. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must seek permission from the School Business Manager or the Headteacher.
- Secure passwords, as outlined in our annual Cyber Security Training, are used to access school computers, laptops and other electronic devices. **Staff and pupils are reminded that they should not reuse passwords from other sites.**
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy / ICT policy / acceptable use agreement / policy on acceptable use])
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
    - **Entry controls:** Any stranger seen in entry-controlled areas should be reported to Premises and/or the School Business Manager or a member of SLT.
    - **Secure lockable desks and cupboards:** Desks and cupboards should be kept locked if they hold confidential information of any kind (Personal information is always considered confidential).
    - **Methods of disposal:** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.
    - **Equipment:** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
    - **Working away from the school premises – working online from home:** Data must not be downloaded onto a personal device and USB stick drives should never be used for personal data.
    - **Document printing:** Documents containing personal data must be printed securely either by using the Follow-Me secure printers/copiers or by using a local printer near your workstation. Items printed on the latter must be collected immediately and not left on the printer.

Any breach of these security measures may be subject to disciplinary action.

17. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees in form of a 'Disposal Certificate' that it complies with data protection law.

18. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

When appropriate, the DPO will report the data breach to the ICO within 72 hours after becoming aware of it.

For further guidance, please visit:

Personal data breaches: a guide | ICO

19. Complaints

We take any complaints about how we collect and use personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance.

You can make a complaint to us at any time by contacting our Data Protection Officer (contact details under 5.2. of this policy)

Upon receiving a complaint, we will:

- Acknowledge receipt of the complaint within 30 days of receiving it
- Without undue delay, take appropriate steps to respond to the complaint, including:

  - Making appropriate enquiries based on the circumstances of the complaint
  - Keeping the complainant informed on the progress of the investigation

- Without undue delay, inform the complainant of the outcome of the investigation

20. Training

All staff and governors are provided with Data Protection / Cyber Security Training as part of their induction process.

Data Protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

21. Monitoring arrangements

The School Business Manager is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the Full Governing Board.

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies. This document has now been withdrawn, however the DfE's latest guidance does not include data protection in its list of statutory policies for maintained schools or academies, including free schools, however it is a legal requirement that Sydenham School has a Data Protection Policy and procedures in place.

22. Links with other policies

This data protection policy is linked to our:

- Safeguarding Policy
- Acceptable Use Policy
- Freedom of Information Publication Scheme
- Privacy notices

Appendix 1: Data Breach Procedure & Reporting Template

1. **Policy Statement**

1.1 Sydenham School is committed to the protection of all **personal data** and **special category personal data** for which we are the **Data Controller**.

1.2 The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.

1.3 All **staff** and **governors** must comply with this policy when **processing personal data** on our behalf. **Any breach of this policy may result in disciplinary or other action.**

1.4 This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

2. **About this policy**

2.1 This policy informs all of **staff** and **governors** on dealing with a suspected or identified data security breach.

2.2 In the event of a suspected or identified breach, the school must take steps to minimise the impact of the breach and prevent the breach from continuing or reoccurring.

2.3 Efficient internal management of any breach is required, to ensure swift and appropriate action is taken and confidentiality is maintained as far as possible.

2.4 The School must also comply with its legal and contractual requirements to notify other organisations including the Information Commissioners Office ("the ICO") and where appropriate **data subjects** whose **personal data** has been affected by the breach. This includes any communications with the press.

2.5 Failing to appropriately deal with and report data breaches can have serious consequences for the school and for **data subjects** including:

- identity fraud, financial loss, distress or physical harm;
- reputational damage to Federation; and
- fines imposed by the ICO.

3. **Definition of data protection terms**

3.1 All defined terms in this section of the policy are indicated in **bold text**, and have the same definition as set out within the main Data Protection Policy.

4. **Identifying a Data Breach**

4.1 A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4.2 This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records.

4.3 A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data.

5. **Internal Communication**

Reporting a data breach upon discovery

5.1 On finding, suspecting or causing a breach, or potential breach, staff / governors or data processor must immediately contact the Data Controller in the first instance.

Data Controller – Martin Brooks m.brooks@sydenham.lewisham.sch.uk

5.2 They will complete a first investigation and will pass the details on to our DPO:

School Business Manager – Simone McAllister s.mcallister@sydenham.lewisham.sch.uk

She can be contacted on either the email above or on 020 8699 6731.

5.3 The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully lost, destroyed, corrupted or disclosed.

5.4 The DPO will alert the Headteacher and the Chair of Governors.

5.5 The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant members of the workforce or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).

5.6 The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

5.7 The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the federation becoming aware of the breach.

5.8 The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored appropriately in the school's records.

5.9 Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible.
- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

5.10 If all the above details are not yet known, the DPO will report as much as they can within 72 hours.The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

5.11 The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

5.12 The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

5.13 Records of all breaches will be stored securely in the school's IT records.

5.14 The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

5.15 Members of our workforce who fail to report a suspected data breach could face disciplinary or other action.

6. **Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on containing the breach and recovering any data, especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

7. **Sensitive information being disclosed via email (including safeguarding records)**

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff who receive personal data sent in error must alert the sender and the School Business Manager / Data Controller as soon as they become aware of the error as set out in the email attachment.

If the sender is unavailable or cannot recall the email for any reason, the School Business Manager / Data Controller will ask the IT providers to recall it.

In any cases where the recall is unsuccessful, the School Business Manager / Data Controller will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way in line with the email attachment instruction.

The School Business Manager / Data Controller will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

The School Business Manager / Data Controller will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

8. **In the event that non-anonymised pupil exam results or staff pay information being shared with governors**

If non anonymized information is accidentally made available to unauthorised individuals, the person who has authorised the disclosure must attempt to rectify the disclosure as they become aware of the error.

Governors who receive personal data sent in error must alert the person who made the disclosure and the School Business Manager / Data Controller as soon as they become aware of the error.

The person who made the disclosure or any other member of staff who is aware should notify the School Business Manager / Data Controller.

The School Business Manager / Data Controller will contact the relevant unauthorised individuals who received information, explain that the information was given in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The School Business Manager / Data Controller will ensure we receive an appropriate response of confirmation from all the individuals who had access to the data, confirming that they have complied with this request.

The School Business Manager / Data Controller will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

9. **In the event that a school laptop containing non-encrypted sensitive personal data being stolen or hacked**

- Procedures should be in place that such information is encrypted, and password protected
- The person who is the victim of the theft or hacking or any other member of staff who is aware should notify the police
- The person who is the victim of the theft or hacking or any other member of staff who is aware should notify the School Business Manager / Data Controller.
- If non anonymized information is available on the stolen item, the police will be informed of the risk of breach.
- The School Business Manager / Data Controller will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted and report these findings to the police.

10. **In the event the school's cashless payment provider being hacked and parents' financial details stolen**

- The school will report any breach to the third-party provider as soon as they become aware and confirm the provider will comply with their privacy notice and breach procedures and any other legal duties they have.
- The School Business Manager / Data Controller will require and receive written confirmation that the third-party provider is acting appropriately and in line with the GDPR.
- The School Business Manager / Data Controller will contact the relevant individuals following the procedures above whose data has been stolen and let them know of the actions taken by the police and the provider to protect and recover their information.
- The School Business Manager / Data Controller will ensure we receive an appropriate response of confirmation from the third-party provider they have complied with their duties.
- The School Business Manager / Data Controller will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- Additional steps could include:
    - remote deactivation of mobile devices;
    - shutting down IT systems;
    - contacting individuals to whom the information has been disclosed and asking them to delete the information; and

- recovering lost data.

11. **External communication**

All external communication is to be managed and overseen by the DPO and headteacher.

12. **Law Enforcement**

12.1 The DPO and/or the Headteacher will assess whether the data breach incident requires reporting to any law enforcement agency, including the police. This will be informed by the investigation and analysis of the data breach, as set out above.

12.2 The DPO and/or Headteacher shall coordinate communications with any law enforcement agency.

13. **Other Organisations**

13.1 If the data breach involves personal data which we process on behalf of other organisations then we may be contractually required to notify them of the data breach.

13.2 The School will identify as part of its investigation of the data breach whether or not this is the case and any steps that must be taken as a result.

14. **Information Commissioner's Office**

14.1 If School is the data controller in relation to the personal data involved in the data breach, which will be the position in most cases, then the School has 72 hours to notify the ICO if the data breach is determined to be notifiable.

14.2 A data breach is notifiable unless it is unlikely to result in a risk to the rights and freedoms of any individual. The DPO will make an assessment of the data breach against the following criteria taking into account the facts and circumstances in each instance:

- The type and volume of personal data which was involved in the data breach;
- whether any special category personal data was involved;
- the likelihood of the personal data being accessed by unauthorised third parties;
- the security in place in relation to the personal data, including whether it was encrypted;
- the risks of damage or distress to the data subject.

15. **Other supervisory authorities**

If the data breach occurred in another country or involves data relating to data subjects from different countries then the DPO will assess whether notification is required to be made to supervisory authorities in those countries.

16. **Data Subjects**

16.1 When the data breach is likely to result in a high risk to the rights and freedoms of the data subjects then the data subject must be notified without undue delay. This will be informed by the investigation of the breach by the school.

16.2 The communication will be coordinated by the School Business Manager / Data Controller and will include at least the following information:

- a description in clear and plain language of the nature of the data breach;
- the name and contact details of the DPO;
- the likely consequences of the data breach;

- the measures taken or proposed to be taken by the school to address the data breach including, where appropriate, measures to mitigate its possible adverse effects.

17. **There is no legal requirement to notify any individual if any of the following conditions are met:**

- appropriate technical and organisational protection measures had been implemented and were applied to the data affected by the data breach, in particular, measures which render the data unintelligible to unauthorised persons (e.g. encryption);
- measures have been taken following the breach which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise;
- it would involve disproportionate effort to contact individuals. In which case a public communication or similar equally effective measure of communication to the data subjects shall be issued.

For any data breach, the ICO may mandate that communication is issued to data subjects, in which case such communication must be issued.

18**. Press**

18.1 Staff shall not communicate directly with the press and shall treat all potential data breaches as confidential.

18.2 All press enquiries shall be directed to the Headteacher.

19. **Producing an ICO Breach Notification Report**

19.1 All staff and governors are responsible for sharing all information relating to a data breach with the DPO, via the School Business Manager / Data Controller, which will enable a Breach Notification Report Form to be completed.

19.2 When completing the attached Breach Notification Report Form (Appendix 2) all mandatory (*) fields must completed, and as much detail as possible should be provided.

19.3 The DPO may require individuals involved in relation to a data breach to each complete relevant parts of the Breach Notification Form as part of the investigation into the data breach.

19.4 If any staff or governor is unable to provide information when requested by the DPO, then this should be clearly reflected in the Breach Notification Form together with an indication as to if and when such information may be available.

19.5 In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

19.6 If reportable, the ICO requires that the School send the completed Breach Notification Form to casework@ico.org.uk, with 'Personal data breach notification' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

20. **Evaluation and response**

20.1 Reporting is not the final step in relation to a data breach. The School will seek to learn from any data breach.

20.2 Therefore, following any breach an analysis will be conducted as to any steps that are required to prevent a breach occurring again. This might involve a step as simple as emailing all relevant members of our workforce to reinforce good practice, or providing additional training, or may in more serious cases require new technical systems and processes and procedures to be put in place.

21. Sydenham Breach Report template.docx