

ST. MARK'S CE SCHOOL
ONE SCHOOL - SERVING ALL - THROUGH EXCELLENCE

Data Protection Policy and Procedure

Policy Statement, Procedures and Guidelines

Policy Date: Spring 2025

Review: Spring 2027

Contents

1. Aims.....	2 2.
Legislation and guidance	2 3.
Definitions	3 4.
The data controller.....	4 5.
Roles and responsibilities	4 6.
Data protection principles.....	5 7.
Collecting personal data.....	5 8.
Sharing personal data.....	7 9.
Subject access requests and other rights of individuals	7 10.
Parental requests to see the educational record	9 11.
Biometric recognition systems.....	9 12.
CCTV.....	10 13.
Photographs and videos	10 14.

Artificial Intelligence (AI).....	10 15.
Data protection by design and default	11 16.
Data security and storage of records.....	13 17.
Disposal of records	13 18.
Disposal of assets.....	13 19.
Personal data breaches	14 20.
Training.....	14 21.
Monitoring arrangements	14 22.
Links with other policies	14
Appendix 1: Personal data breach procedure	15

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with the UK data protection law.

Data Protection Act 2018 (DPA 2018)).

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:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

2

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

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

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.

3

Data controller A person or organisation that determines the purposes and the means of processing of personal data.

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.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data protection officer

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.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Judicium Consulting Limited and is contactable via:-

Telephone: 020 3326 9174

Address: 72 Cannon Street

London

EC4N 6AEE

E-mail: dataservices@judicium.com

Our Data Protection/Compliance Lead, who deals with data protection management day to day is Mr C Lovett and is contactable via:-

Telephone: 023 8077 2968

Address: St. Mark's CE School,

Stafford Road

Shirley

Southampton

SO15 5TE

E-mail: info@st-marks-southampton.org.uk

4

5.3 Headteacher

The headteacher acts as the representative 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 (Who may seek further clarification from a variety of sources):
 - 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 European Economic Area
- 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

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- 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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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
- 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 or exercise its official authority**
- 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
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

5

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.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 data protection law
 - Establish a contract with the supplier or contractor 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

We will also share personal data with law enforcement and government bodies where we are legally required to do so. This includes for the purposes of Operation Endeavour, which shares information with Hampshire Constabulary. Operation Endeavour, and the lawful powers that place a duty on us, are detailed in our Privacy notice which can be found on our School website.

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 internationally, we will do so in accordance with data protection law.

Process for Pupil Record Transfer when a child leaves.

- CTF system to be used for computer transfer of details
- Children to take their own books wherever possible
- If books or any pupil records do need to be sent they should be secured in a bag and then an envelope, the envelope must not be overloaded
- The form re contents of the envelope must be completed and sent
- Hermes or recorded delivery must be used as both of these systems allow the parcel to be tracked. For Southampton schools the black bag can be used but again the records form must be included, chased and obtained
- The parcel must be tracked and when it has arrived a call made to the school to ensure it has arrived in a good condition, in addition the form re acceptance of records must be chased and obtained
- CPOMs records must be transferred via the CPOMs system wherever possible (call made to the school to ascertain if they have the system when we check a pupil has arrived at the school and is on roll) NB Other pupil names to be removed
 - Before downloading any information from CPOMS please ensure that you have got permission to do so from a DSL. When downloading information is it easier to copy (by highlighting) from CPOMS and pasting into Word. Once pasted the file must be saved and encrypted with a password, unless it is being sent via AnyComms. To password protect follow the steps below). If sending this via e-mail or unsecured and non-encrypted transfer you must send the password separately or via a phone call.
- If this system is not possible the record should be downloaded & the details saved in a password protected document
- The password should be given to the school via phone to ensure the right person is getting the details

9. Subject access requests and other rights of individuals

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 DPO. **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 below the age of 12 are generally not 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 our school may 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.

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 our 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 or they can seek to enforce their subject access right through the courts.

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

- Object to processing which 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

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 (for example, via our online registration form) from at least one 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 be searched for manually instead of using their fingerprint.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data

already captured is deleted.

9

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 for health and safety, the detection, prevention and investigation of crime and also for the safeguarding of stakeholders. 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 at all access points to the site. Our system retains footage for 34 days and then this is overwritten.

In some instances, the footage may be shared with law enforcement agencies and for the purposes of safeguarding our pupils and other stakeholders. Please also see our CCTV Policy and Procedure for further information.

Any enquiries about the CCTV system should be directed to Stephanie Bryant via the school contact details. Telephone: 023 8077 2968. E-mail: info@st-marks-southampton.org.uk. Address: St. Mark's CE School, Stafford Road, Shirley, Southampton. SO15 5TE.

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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.

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 (and 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 our 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, except where appropriate, first name and class, as appropriate.

See our child protection and safeguarding policy for more information on our use of photographs and videos in conjunction with our Social Media and E-Safety and Digital Technology Policy.

We may use photographs and videos to record pupils learning in school to comply with our duties to keep a record of pupil's educational attainment.

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. St. Mark's CE 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.

This section outlines the acceptable use of Artificial Intelligence (AI) tools, within our school. It aims to ensure that AI is used responsibly, ethically, and in a manner that enhances learning and administrative processes. It applies to all staff who use AI for school-related activities.

Staff should register with their school email account to receive potential subscription benefits.

Introduction

1. **Educational Enhancement:** AI tools could be used to support and enhance educational experiences but should not replace traditional teaching methods.
 - *Example:* Staff can use TeachMateAI (a suggested platform) to support lesson planning but should still engage with pupils through discussions and hands-on activities.
2. **Ethical Use:** All users must adhere to ethical guidelines, ensuring AI is used in a manner that respects privacy, promotes fairness, and avoids harm.
 - *Example:* Staff should not use AI to generate inappropriate, harmful, offensive content or false information about someone to bully in any form of communication.
3. **Compliance:** Users must comply with all relevant laws, regulations, and school policies when using AI tools.
 - *Example:* Staff should ensure that any AI-generated content complies with copyright laws and does not plagiarize existing materials.

Expectations for the use of AI Tools

- **Confidentiality:** Staff must not input any confidential or sensitive data into AI tools.
 - *Example:* Do not enter any personal information, such as personal pupil information or medical records into Microsoft Copilot Chat (a possible platform).
- **Data Protection:** Follow the school's data protection policies and guidelines to ensure the security of personal data.
 - *Example:* Use secure channels for any necessary data transfers and ensure that AI tools are used in compliance with GDPR.
- **Awareness:** Be aware of the data that AI tools collect and how it is used.
 - *Example:* Understand that AI tools may collect usage data to improve their services, and ensure this data is handled according to privacy laws.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, St. Mark's CE 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 European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure

14.1 Data Protection Impact Assessments (DPIA)

We will carry out a DPIA when:

- Using new technologies; and
- The processing is likely to result in a high risk to the rights and freedoms of individuals

Processing that is likely to result in a high risk includes (but is not limited to):

- Systematic and extensive processing activities, including profiling and where decisions have legal effects, or similarly significant effects, on individuals
- Large-scale processing of special categories of data or personal data relating to criminal convictions or offences
- Large-scale, systematic monitoring of public areas (such as CCTV)

Criteria

Pages 9 to 11 of the working party guidelines from the ICO set out criteria to consider when deciding whether a DPIA is needed. In most cases, meeting 2 criteria would require us to carry out a DPIA, although we will choose whether to conduct a DPIA if our processing meets only 1.

The criteria are:

1. Evaluation or scoring
2. Automated decision making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale
6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself prevents data subjects from exercising a right or using a service or contract

Process

We will carry out an DPIA prior to the data processing and will record our assessment on a template form

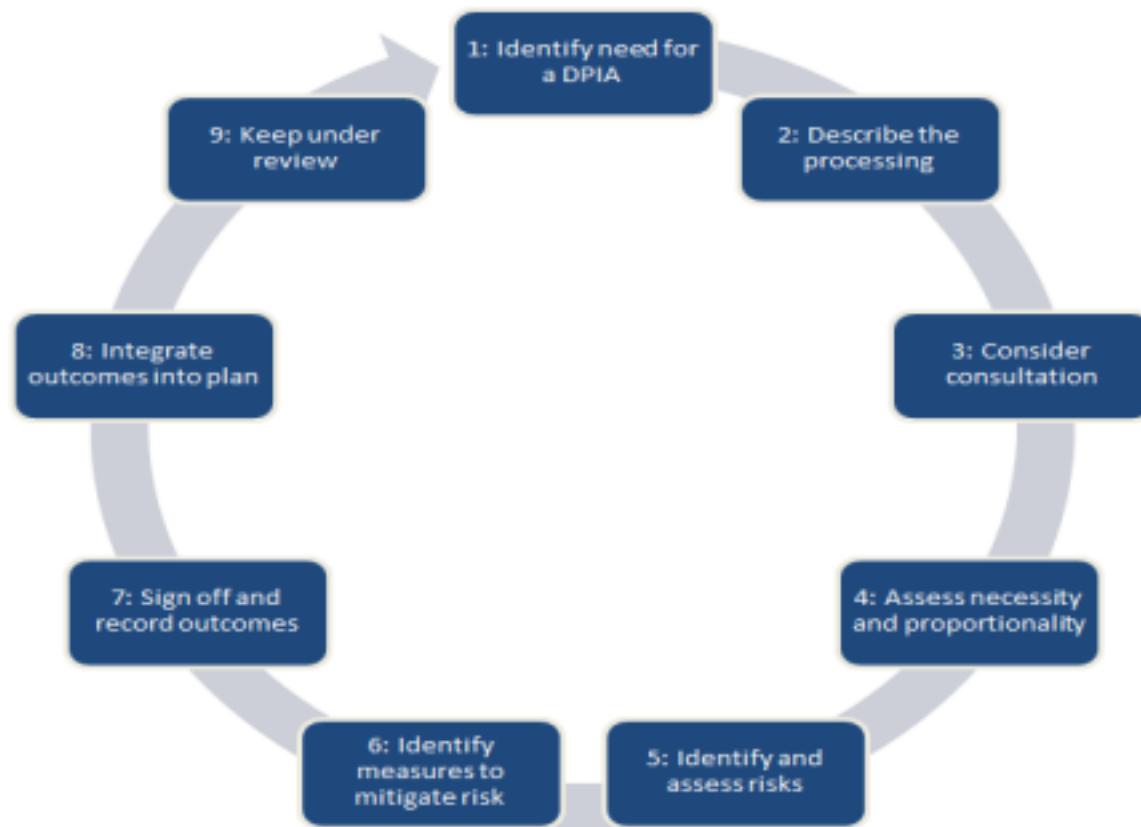
which is located on the google drive and is accessible to all staff.

A DPIA will include:

12

- A description of the processing operations and purposes, including, where applicable, the legitimate interests pursued by the data controller
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An assessment of the risks to individuals
- The measures in place to address risk, including security and to demonstrate that you comply

A cycle process is as follows.



16. Data security and storage of records

This section should be read in conjunction with the E-Safety and Digital Technology Policy, that give further information and guidance. 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:

- We will not allow staff to use personal devices within school for the processing of personal and special category data.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept secure or 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 sign it in and out from the DPO or the

Systems Manager following authorisation to take it off site

- Passwords that are at least 8 characters long containing capital and lowercase letters, numbers and a least 1 special character 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 and should keep these secure. Further information on password security can be found in the E-Safety and Digital Technology Policy

13

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- When attaching a document that contains personal data to an email we will enable password protection on the document. If these are sent outside of the school the password will not be sent with the file, but via a separate means
 - To set a password on your Word, Excel or PowerPoint file click **File > Info > Protect Document > Encrypt with Password**. You'll be prompted to create a password, then to confirm it. After you've added a password to your file you'll want to be sure to save the file to make sure the password takes effect.
 - To remove the password open the file, which will require the current password, go to **File > Protect Document > Encrypt with Password**. Delete the password and click OK. Be sure to save your file to make that change permanent.
- 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 e-safety policy and 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)

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 that it complies with data protection law. (See section 18 for IT equipment)

18. Disposal of assets

Please read this in conjunction with our Write-Off Policy. Written-off items and other major assets/resources, which are surplus to requirements, unserviceable or obsolete should be disposed of by scrapping, recycling or destroying especially when they contain personal data.

Where possible, items should be disposed of in an environmentally appropriate way, including recycling.

For our IT assets, which in most cases will contain data, these are disposed of securely using a company called Jamie's Computers (a charity), that wipes all data from any device and recycles it, allowing it to be reused or used as parts to keep other devices running. Jamie's Computers uses secure data erasure software from Blancco, using a Garner Data Eliminator HD-3WXL which is performed to UK HMG InfoSec Standard 5.

19. 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, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

14

20. Training

All staff and governors are provided with data protection 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 DPO is responsible for monitoring and reviewing this policy in conjunction with the Data Protection/Compliance Lead.

This policy will be reviewed annually and approved by the full governing board.

22. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E-safety and Digital Technology policy
- Acceptable use of ICT
- Privacy Notices
- Safeguarding policy
- CCTV Policy
- Write-Off Policy
- Social Media and Networking Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO by contacting them directly if they are in school. If they are not, an urgent call or e-mail needs to be sent to their personal e-mail account with the subject 'Urgent – Data Protection Breach'.
- 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
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO will alert the Executive Headteacher and the Chair of Governors if appropriate to do so.
- The breach will be logged on our GDPR management system GDPRiS and the relevant form will be completed, which can be delegated to the Data Protection/Compliance Lead and signed off by the DPO.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/) available at <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/>
- 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 on the GDPR management system (GDPRiS) and in paper form in the locked filing cabinet of the Data Protection/Compliance Lead.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](https://ico.org.uk/report-a-breach/), or through their breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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
 - If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. 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
 - Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach ○

- 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

As above, any decision on whether to contact individuals will be documented by the DPO.

- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- 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)

Records of all breaches will be stored on our GDPR management system GDPRiS and in paper format in the Data Protection Lead's locked filing cabinet.

- The DPO and Executive Headteacher, and where necessary any other member of staff, will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Executive Headteacher will meet regularly throughout the year, a minimum of twice yearly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below examples of the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information, however this is not an exhaustive list. We will review the effectiveness of these actions and amend them as necessary after any data breach.

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 DPO as soon as they become aware of the error
 - If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department or external IT Support (Soft Egg 0800 999 1212) to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO 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

A school laptop containing non-encrypted sensitive personal data being stolen or hacked

- Ascertain, where possible the data that was present on the device. If special category data (sensitive information) was present and the extent of what information was contained within it.

- Request that our ICT department or external IT Support (Soft Egg 0800 999 1212) do all that it can to remotely secure the device or remove the data contained on the device.
- Ensure that no further breaches are possible through firewalls or security features by contacting appropriate ICT support (inc. Soft Egg, TalkStraight via ICT Strategy).

17

- The appropriate authorities (i.e. the police) will be alerted to the breach and loss of this device (whether stolen or otherwise) as necessary and request their help in locating the device.
- Where possible attempt to track the location of the device.
- Where possible ensure that as much personal data is stored securely on our cloud based solution and not physically on devices, including reminding staff of their responsibility to refrain from downloading data onto devices, but working online instead.
- The DPO 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

