South Grove Primary School
Data Protection Policy
GDPR

Date Governors Agreed:	May 2018		
Date to be reviewed:	May 2019		
Head Teacher:		**Date:**	
		Date:	

Contents

1. Introduction

South Grove Primary School uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

The school has a legal responsibility to comply with data protection legislation and other statutory provisions relating to the way in which it holds and processes personal data. The school, as a corporate body, is named as the Data Controller under the Act.

The school is required to 'notify' the Information Commissioner of the processing of personal data. This information is included in a public register which is available on the Information Commissioner's website at:
http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/keeping_the_register.aspx

Every member of staff, member of the Governing Body, contractors, and partners of the School that hold its' personal information has to comply with the law when managing that information. Schools also have a duty to issue a Privacy Notice to all pupils/parents and its' employees; these provide details of information collection and held, why it is held and the other parties to whom it may be passed on.

As data controller personal data collected about staff, pupils, parents, governors, visitors and other individuals that is collected and held must be processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) as is currently set out in the Data Protection Bill.

2. Aims

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

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

3. Scope of the Policy

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the school. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. Under the GDPR, personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

The School collects a large amount of personal data every year including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

4. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice 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.

5. Definitions

Term	Definition
Consent	An agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Privacy Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the 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.

Data Protection Officer (DPO)	Is responsible for monitoring our compliance with data protection law.
Data Subject	A living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be national or residents of any country and may have legal rights regarding their Personal Data.
Data Users	Employees whose work involves processing personal data. Data users
Personal data	Any information relating to an identified, or identifiable natural person, individual. An identifiable natural person is one who can be identified, directly or indirectly. In particular, by reference to an identifier. 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.
Personal Data Breach	Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Processing	Is any activity which is performed on personal data such as collection, recording, organization, structuring, adaptation or alteration, using, storage, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
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

6. 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 as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

7. Roles and responsibilities

This policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present pupils, employees, workers, supplier contacts, website users or any other Data Subject.

Staff and those working on our behalf

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf.

You must read, understand and comply when Processing Personal Data on our behalf and attend training on its requirements. This policy sets out what we expect from you in order for the School to comply with applicable law. Your compliance with this policy is mandatory. You must also comply with all related Policies and guidelines given. Staff who do not comply with this policy may face disciplinary action.

7.1 Governing Body

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

7.2 Head Teacher

The Head Teacher has overall operational responsibility on a day-to-day basis for the implementation of the school's policies and procedures.

7.3 Education Data protection officer

The Education Data Protection Officer (EDPO) 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 Body and, where relevant, report to the Governing Body their advice and recommendations on school data protection issues.

The EDPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the EDPO's responsibilities are set out in their job description.

Our School's **DPO is Rosette Doxon**, our School's Business Manager and is contactable via South Grove Primary School, school@southgrove.waltham.sch.uk

The school's support **and EDPO is Adeyemi Tiamiyu** and is contactable via The London Borough of Waltham Forest via edposervice@walthamforest.gov.uk

7.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Ensuring that personal data held is accurate and up to date
- Ensuring that personal data held is not misused, lost or unlawfully disclosed
- Informing the school of any changes to their personal data, such as a change of address
- **All staff must contact the DPO in the following circumstances:**
    - With any questions about the operation of this policy, the purposes for which data may be used; retaining personal data; disclosing 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 or wish to process for a different purpose than the one that the data was obtained
    - 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
    - Where they propose to engage in any activity that affects the rights of privacy of any individual i.e. where there is a legal obligation to carry out a Privacy Impact Assessment
    - Where they are unsure about what security or other measures they need to implement to protect Personal Data
    - If they need any assistance dealing with any rights invoked by a Data Subject
    - 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
    - Where they are entering into contracts involving the processing of personal data by another organisation
    - Where staff have concerns that this policy is not being followed by others they should report this immediately to the DPO. Where they wish to raise this formally they may do so under the Schools' Policy and Procedure for reporting of Data Protection Infringements by Employees.

8. Personal 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 (Lawfulness, Fairness and Transparency).
- Collected for specified, explicit and legitimate purposes (Purpose Limitation).
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (Data Minimisation).
- Accurate and, where necessary, kept up to date (Accuracy).
- Kept for no longer than is necessary for the purposes for which it is processed (Storage Limitation).
- Processed in a way that ensures it is appropriately secure (Security, Integrity and Confidentiality).
- Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

The school is committed to maintaining the data protection principles at all times. This means that the school will:

- Inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice
- Check the quality and accuracy of the information held
- Apply the records management policies and procedures to ensure that information is not held longer than is necessary
- Ensure that when information is authorised for disposal it is done appropriately
- Ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- Only share personal information with others when it is necessary and legally appropriate to do so
- Set out clear procedures for responding to requests for access to personal information known as subject access request
- Train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

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

9. Collecting personal data

9.1 Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows us only to process personal data where we have one 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 e.g. 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, known as the Public Task
- The data needs to be processed for the **legitimate interests** of the school 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**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

9.2 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.

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 Records Management and Retention Policy.

You may wish to refer instead to the Information and Records Management Society's toolkit for schools.

10. Sharing personal data

We will not normally share personal data with anyone else without consent, but may do so where:

- It is necessary for the performance of our Public Task
- 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 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 European Economic Area, we will do so in accordance with data protection law.

We may enter into Information Specific Sharing Agreements with other public bodies for the purposes outlined above.

11. Subject access requests and other rights of individuals

11.1 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. These rights include:

- 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
- 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

Where an individual exercises their rights of subject access this will be dealt with under the schools Subject Access Request Policy and Procedure.

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

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the school's DPO.

11.2 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.

11.3 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 15 days of receipt of the request
- 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 will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

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

11.4 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing purpose
- Challenge processing which has been justified on the basis of our legitimate interests or public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

- Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else
- Be notified of a personal data breach in certain circumstances which is likely to result in high risk to their rights and freedoms
- 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 **Data Protection Officer**, Rosette Doxon via School@southgrove.waltham.sch.uk

12. 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.

13. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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 Keir Management Services and SSO Mrs Marion Howe.

14. 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.

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.

See our Child protection and Safeguarding Policy for more information on our use of photographs and videos.

15. Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

We keep and maintain accurate records reflecting our Processing. These records include clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing

purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

16. Accountability, 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 EDPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge, with support from an SLA with the LA appointed EDPO
- 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 privacy 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 EDPO 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
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and EDPO 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

17. 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, pinned to notice/display boards, 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 school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software/Remote access 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)

18. 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.

19. Personal data breaches

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

A personal data breach is more than just losing personal data. It is a breach of security leading to the accidental or lawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. The Schools Personal Data Breach Procedure and take all steps we can to remedy the breach that has occurred.

When appropriate, we will report the data breach to the ICO within 72 hours. 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

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. Review and Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated as and when necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the Full Governing Body.

Note: the 2-year review frequency here reflects the information in the Department for Education's advice on statutory policies. While the GDPR and Data Protection Act 2018 (when in place) are still new and schools are working out how best to implement them. Therefore, the school will be reviewing the data protection policy annually, and then extend this to every 2 years once we are confident with our arrangements.

22. Contacts:

Further specialist information and advice may be sought from the **Schools Data Protection Officer**:

Rosette Doxon, Data Protection Officer for South Grove Primary School

Email: school@southgrove.waltham.sch.uk

Or

For help or advice on this policy please contact:

Adeyemi Tiamiyu

Education Data Protection Officer via

Education Data Protection Service Team

Governance & Law

London Borough of Waltham Forest

Email: edposervice@walthamforest.gov.uk

23. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy (Acceptable Use of ICT Policy)
- Child Protection and Safeguarding Policy

Further school policies can be found via the web link below:

http://southgrove.waltham.sch.uk/page.cfm?pageid=8

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
- 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 Head Teacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out 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
- 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.
- 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 school's administration computer system.
- 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
- 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
- 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
- The DPO will 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 and documented decisions are stored on the school's administration computer system.

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

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 breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

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 Technician to recall it*
- *In any cases where the recall is unsuccessful, the DPO 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*
- *The DPO will ensure we receive 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*

Other types of breach that you might want to consider could include:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-anonymised pupil exam results or staff pay information being shared with Governors*
- *A school laptop containing non-encrypted sensitive personal data being stolen or hacked*
- *The school's cashless payment provider being hacked and parents' financial details stolen*