

Data Protection Policy

Limehurst Primary School



Approved by:	Diane Wright	Date: 20.4.20
Last reviewed on:	25.5.18	
Next review due by:	20.4.22	

Contents

1. Aims	2
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	5
8. Sharing personal data.....	8
9. Subject access requests and other rights of individuals.....	8
10. Parental requests to see the educational record	11
11. CCTV	12
13. Photographs and videos	12
14. Data protection by design and default	13
15. Data security and storage of records.....	13
16. Disposal of records	14
17. Data breaches	14
18. Training.....	14
19. Monitoring arrangements.....	14
Appendix 1: Personal data breach procedure	15
2: Data Amendment Request Process Flowchart.....	19
3: The Independent Inquiry into Child Sexual Abuse.....	20

1. Aims

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 \(EU\) 2016/679 \(GDPR\)](#) and the [Data Protection Act 2018 \(DPA 2018\)](#).

Everyone has rights with regard to the way in which their personal data is handled. During the course of the School's activities it collects, stores and processes personal data about staff, pupils, their parents, suppliers and other third parties, and it is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Any breach of this Policy may result in disciplinary action.

This Policy sets out the basis on which the School will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It does not form part of any employee's contract of employment and may be amended at any time.

The policy meets the requirements and expectations of the General Data Protection Register introduced in law as of the 25th May 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 GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#).

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.

3. Definitions

TERM	DEFINITION
Personal data	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none">› Name (including initials)› Identification number› Location data› Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none">› 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	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>

TERM	DEFINITION
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 pays its data protection fee to the ICO, as 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 School has appointed Diane Wright as Data Protection Officer(DPO) and is contactable via dwright@limehurst.oldham.sch.uk, who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the Act. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the 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.

They will report 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.

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:
 - 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

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 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 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**

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.

Types of Personal Data Processed by The School

Personal data covers both facts and opinions about an individual. The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including, by way of example:

- ✓ Names, addresses, telephone numbers, email addresses and other contact details
- ✓ Bank details and other financial information, e.g. about parents who pay fees to the School
- ✓ Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks
- ✓ Where appropriate, information about individuals' health, and contact details for their next of kin
- ✓ References given or received by the School about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- ✓ Images of pupils (and occasionally other individuals) engaging in School activities, and images captured by the School's CCTV system (in accordance with the School's policy on taking, storing and using images of children)
- ✓ Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another School, or other professionals or authorities working with that

individual), or collected from publicly available resources

Sensitive Personal Data

The School may, from time to time, need to process sensitive personal data regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the School with the explicit consent of the appropriate individual, or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

Use of Personal Data by The School

The School will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- ✓ For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents
- ✓ To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the School community
- ✓ For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the School's performance;
- ✓ To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil has attended or where it is proposed they attend
- ✓ To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School
- ✓ To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips;
- ✓ To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's Computing and Acceptable Use and E-safety Policies
- ✓ To make use of photographic images of pupils in School publications, on the School website and (where appropriate) on the School's social media channels in accordance with the School's policy on taking, storing and using images of children
- ✓ For security purposes, and for regulatory and legal purposes (for example safeguarding and child protection and health and safety) and to comply with its legal obligations; and
- ✓ Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School

Keeping in Touch and Supporting the School

The School will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School may also:

- ✓ Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the School community.
- ✓ Contact parents and/or alumni by post and email in order to promote and raise funds for the School and, where appropriate, other worthy causes

- ✓ Should you wish to limit or object to any such use, or would like further information about them, please contact the DPO in writing

If we want to use personal data for reasons other than those given, 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.

School Website

The school has a page on its website to ensure that its approaches, policies and practices in relation to data are transparent. It will provide parents with information that may be relevant to their data concerns. It includes:

- ✓ Information about the school's Data Protection Officer (name, contact details etc)
- ✓ Copies of relevant policies
- ✓ Data review and amendment request forms
- ✓ Process flowcharts
- ✓ Step by step guides
- ✓ Complaints policy

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.

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.

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. Any individual wishing to access their personal data should put their request in writing to the DPO. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within statutory time limits (one month). 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

Individuals have the right under the Act to access their personal data held by the School, subject to certain exemptions and limitations set out in the Act

It should be noted that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may be disclosed), nor any reference given by the School for the purposes of the education, training or employment of any individual.

Unstructured Personal Information

The School will generally not be required to provide access to information held mutually and in an unstructured way.

Further exemptions may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School will also treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment of any pupil. The School acknowledges that an individual may have the right to access a reference relating to them received by the School. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

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

The GDPR states that pupils under the age of 16 are to be considered as 'vulnerable' and therefore are not allowed to amend their own data. As all our pupils are aged 12 and under, all subject access requests from pupils will therefore not be considered.

Only a person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on their behalf. In line with the GDPR, we recognise the following rights in relation to data:

1. Right of Access.

Individuals have the right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to that personal data.

2. Right to Rectification.

Individuals have the right to obtain rectification of inaccurate personal data and the right to provide additional personal data to complete any incomplete personal data.

3. Right to Erasure (“Right to be Forgotten”).

In certain cases, individuals have the right to obtain the erasure of their personal data.

4. Right to Restriction of Processing.

Individuals have the right to obtain a restriction of processing, applicable for a certain period and/or for certain situations.

5. Right to Data Portability.

Individuals have the right to receive their personal data and they have the right to transmit such personal data to another controller.

6. Right to Object.

In certain cases, individuals have the right to object to processing of their personal data, including with regards to profiling. They have the right to object at further processing of their personal data in so far as they have been collected for direct marketing purposes.

7. Right to be Not Subject to Automated Individual Decision-Making.

Individuals have the right to not be subject to a decision based solely on automated processing.

8. Right to Filing Complaints.

Individuals have the right to file complaints about the processing of their personal data with the relevant data protection authorities.

9. Right to Compensation of Damages.

In case of a breach of the applicable legislation on processing of (their) personal data, individuals have the right to claim damages that such a breach may have caused with them.

Exemptions

Certain data is exempted from the provisions of the Act, including the following:

- ✓ The prevention or detection of crime
- ✓ The assessment of any tax or duty
- ✓ Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School
- ✓ Information which might cause serious harm to the physical or mental health of the pupil or another individual
- ✓ Cases where the disclosure would reveal a child is at risk of abuse
- ✓ Information contained in adoption and parental order records
- ✓ Information given to a court in proceedings under the Magistrates’ Courts (Children and Young Persons) Rules 1992
- ✓ Copies of examination scripts; and
- ✓ Providing examination marks before they are officially announced

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.

Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured. The school reserves the right to refuse a request to view or amend data held. This would be rare and only on the following basis :

- ✓ Vexatious requests
- ✓ Where information held maybe required by future legal processes e.g. Child Protection
- ✓ The request would lead to inaccurate and misleading information being recorded
- ✓ The request has come from an individual who has no rights of access

Where the school decides not to adhere to a request it will notify the person who requested of :

- ✓ The reason why the request has been refused
- ✓ Their legal rights of appeal or complaint
- ✓ Their legal rights of referral to the ICO

11. 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 Mr M Roberts, Head Teacher.

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.

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.

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.

See our child protection and safeguarding policy for more information on our use of photographs and videos.

14. 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

15. 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 sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers 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
- 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)

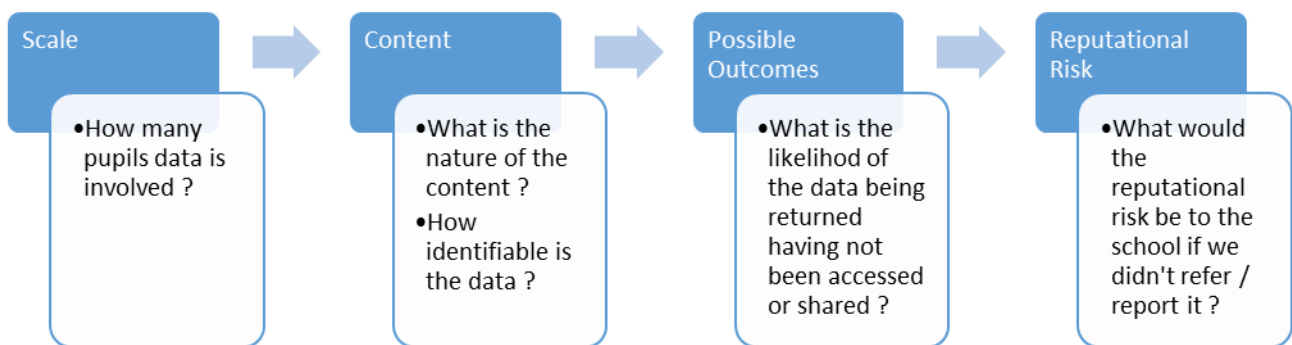
16. Disposal of records

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 except as required by the Independent Inquiry into Child Sexual Abuse (see Appendix 3)

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.

17. Data breaches

The school will make all reasonable endeavours to ensure that there are no data breaches and through its policy and practice endeavour to minimise the risk of a breach. However, in the unlikely event of a suspected data breach, we will follow procedure:



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

18. 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.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. The GDPR requires schools to undertake an evaluation of the data management impact resulting from new initiatives. The school undertakes to review all of its policies (curriculum, safety, statutory etc) to ensure that any potential data management issues are identified and resolved.

This policy will be reviewed every **2 years** and shared with the full governing board as recommended by the Department for Education's [advice on statutory policies](#).

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 headteacher 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 head teacher's computer.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through their breach report line (0303 123 1113), 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:
 - A description, in clear and plain language, of the nature of the personal data breach
 - 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

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

- › 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 relating to the breach
 - 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 the Head Teacher's computer.

- › 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

Actions to minimise the impact of data breaches

We will, where appropriate, take any of 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. For example:

- Special category data (sensitive information) being disclosed via email (including safeguarding records)
- 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

Should an email containing sensitive data be accidentally sent out the following may happen.

- › If sensitive data 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 and any 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
- › The DPO will ask the ICT department to help recall or delete any sensitive information breaches
- › The DPO will contact any unauthorised individuals to explain about any breach 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

Appendix 2: Data Amendment Request Process Flowchart

Transparency and Accountability

To ensure that the school is open and transparent about what data it holds and how it will be managed, the school will bear in mind the following prompts in all that it does :



Appendix 3: **The Independent Inquiry into Child Sexual Abuse**

The Independent Inquiry into Child Sexual Abuse (formerly The Goddard Inquiry) was launched at the beginning of July 2015. The Inquiry is investigating whether public bodies and other non-state institutions have taken seriously their duty of care to protect children from sexual abuse in England and Wales. Judge Goddard made it very clear in her opening statement the importance of retaining records. She wrote to institutions including local authorities and religious organisations on the subject of retaining records but confirmed that the content of those letters should be taken to apply to all institutions which have had responsibility for the care of children.

In view of Judge Goddard's clear direction to institutions not to destroy records, the School will not destroy pupil records after the customary seven year period, as determined by the DPO in accordance with the Data Protection Principles published by the Information Commissioner's Office, but will retain them and all staff records until the Inquiry has concluded. The Inquiry 'trumps' any data protection legislation.