



Data Protection Policy

Policy written and agreed by staff : May 2020

Approved by Governors: 6th May 2020

Signed by DPO:

A handwritten signature in blue ink, appearing to read 'C. P. Benton', written over a horizontal line.

Next Review: May 2022

Data Protection Policy

School Vision

'Love one another as Jesus loved us.' (John 13 v 34-35)

Jesus said, 'Love one another as I have loved you'.

Through God's love and our Christian Values, we encourage each individual to love, respect and value themselves and others.

We encourage and nurture the growth of every individual and their uniqueness so that all flourish and become all that they can be and all that God made them to be.

1. About This Policy

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 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](#).

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. General Statement of Duties

The school is required to process relevant personal data regarding individuals as part of its operation and shall take all reasonable steps to do so in accordance with this policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none">● 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: <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● 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.
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.
--	---

5. 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.

6. 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.

6.1 Governing Body

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

6.2 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.

He 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.

Our DPO is Mr Grahame Benson and is contactable via the school office.

6.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

6.4 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

7. The Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the requirements of the GDPR.

These provide that personal data must be:

- ✓ Fairly and lawfully processed
- ✓ Processed for a lawful purpose
- ✓ Adequate, relevant and not excessive
- ✓ Accurate and up-to-date
- ✓ Not kept for longer than necessary
- ✓ Processed in accordance with the data subject's rights
- ✓ Secure
- ✓ Not transferred to other countries without adequate protection

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

8. 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
- ✓ Past and present pupils' academic, disciplinary, admissions and attendance
- ✓ Records (including information about any special needs), and assessments
- ✓ Where appropriate, information about individuals' health, and contact details for their next of kin
- ✓ 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,
- ✓ 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

9. Sensitive Personal Data

The school may, from time to time, need to process sensitive personal data regarding individuals (pupils, staff and governors). Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sexual orientation, 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.

10. 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 admission and to confirm the identity of prospective pupils and their parents
- ✓ To provide education services (including SEND) and extra-curricular activities; monitoring pupils' progress and educational needs; and maintaining relationships with 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 about past, current and prospective pupils, 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

11. 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, prospectus, 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.

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.

12. Keeping in Touch and Supporting the School

The school will use the contact details of parents 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.

13. Rights of Access to Personal Data ('Subject Access Request')

Individuals have the right under the Act to access to personal data about themselves held by the school, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO, (using appendix B). The school will endeavour to respond to any such written requests as soon as is reasonably practicable and within statutory time limits (one month).

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. (See Sections below on Exemptions and Unstructured Personal Information)

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 11 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 primary aged 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 to 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.

14. The School's Rights to Refuse a Request

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

15. Requests for Amendments of Data

The GDPR establishes the right to amend any data held that is inaccurate or may have a negative or detrimental effect on an individual. Amendments may take the form of updates, redactions or removals. As a school, we believe that before any amendment request is granted the first step is to view the data to ensure that it may be necessary. (See appendix B and C)

16. Charges

The school will not usually make a charge in relation to data viewing or amendment requests. However, it reserves the right to do so where the request is proven to be:

- ✓ Vexatious
- ✓ Excessive

- ✓ Unfounded

17. 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

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.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPO.

18. Unstructured Personal Information

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

19. Whose Rights?

The rights under the Act are those of the individual to whom the data relate. However, the school will, in most cases rely on parental consent to process data relating to pupils (if consent is required under the Act).

Pupils are required to respect the personal data and privacy of others, and to comply with the school's Computing and Acceptable Use and E-safety Policies and any school rules.

20. Disclosure of Information

The school may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. The school confirms that it will not generally disclose information unless the individual has given their consent or one of the specific exemptions under the Act applies. However the school does intend to disclose such data as is necessary to third parties for the following purposes:

- ✓ To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend
- ✓ To publish the results of public examinations or other achievements of pupils of the School
- ✓ To disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of School trips

Where the school receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure.

21. Accuracy

The school will endeavour to ensure that all personal data held in relation to an individual is as up-to-date and accurate as possible. Individuals must notify the School Office of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.

22. Timely Processing

Except as required by the Independent Inquiry into Child Sexual Abuse (see below) the school will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required.

23. Enforcement

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school's complaints procedure and should also notify the DPO.

24. Implementing Data Protection Regulations

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

- Appointing a DPO
- 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
- 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
- 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;
- Regularly conducting reviews and audits to assess 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 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, 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

25. Data Security

25.1. 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 secure when not in use
- Papers containing confidential personal data will kept secure and away from general access
- Where personal information needs to be taken off site, staff and Governors will give due diligence to its security
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops
- 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

The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, and to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties under the Act.

The school must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of or damage to, personal data. Accordingly, no member of staff is permitted to remove personal data from school premises, whether in paper or electronic form and wherever stored, without prior consent of the Head. Where a member of staff is permitted to take data offsite it must be encrypted or satisfy secure arrangements.

25.2 . 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 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.

25.3 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

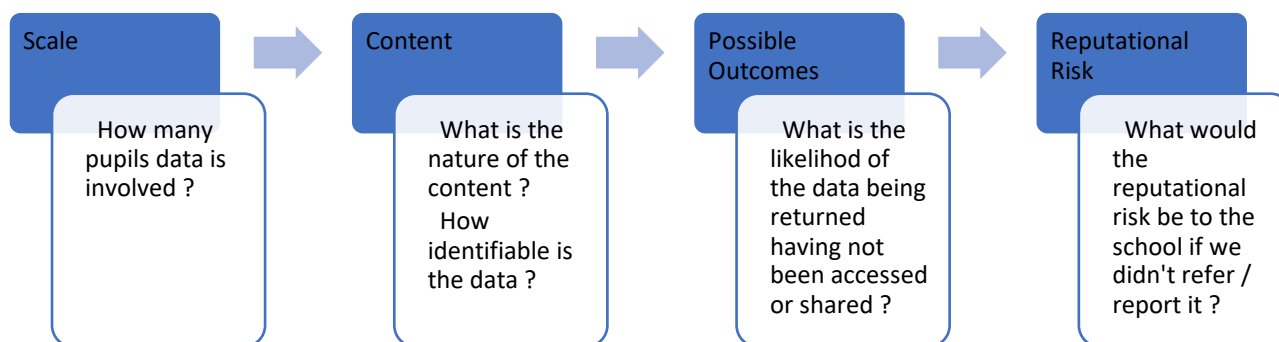
England and Wales. Judge Goddard made it very clear in her opening statement the importance of retaining records. She wrote to institutions including local authorities and religious organisations on the subject of retaining records but confirmed that the content of those letters should be taken to apply 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 if there has been any concern regarding sexual abuse.

26. Data Breaches

The school takes seriously any data breach and will, through its policy and practice endeavour to minimise the risk of a breach. However, in the rare circumstances surrounding a data breach a procedure will be followed. This process can be seen in Appendix A.

The GDPR states that breaches should be referred to the Information Commissioners Office (ICO) within 72 hours of disclosure. However, it is appropriate for our school to consider the following factors before referring to the ICO:



27. 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.

28. Monitoring arrangements

The DPO in conjunction with the Governing Body is responsible for monitoring and reviewing this policy. This policy will be reviewed **every 2 years** and shared with all staff and the full governing body.

29. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding and Child Protection Policy
- E- safety and Acceptable Users policy
- Safer Working Practices
- Privacy Notice

30. Complaints

Complaints related to the management of data in our school will be handled through our existing Complaints Procedure. Copies of which are available on the school website or from the school office upon request.

31. 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:



The school will provide every parent with information in relation to their data rights. In addition, it will also provide every new parent with the school Privacy Notice, which is also available on the school website. This outlines the aspects of data that the school will gather and use, as well as stating their purpose, their 'shelf-life' and where it may be shared. Parents will be asked to acknowledge their understanding of this information and accept the reasoning and processing that may occur.

32. School Website

The school will establish 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 will include:

- ✓ Information about the school's Data Protection Officer
- ✓ Copies of relevant policies
- ✓ Privacy Notice

33. Appendices :

A : Personal Data Breach Procedure

B : Data Review Request Form

C: Data Amendment Request Form

D: Retention of Data Protection Information

Appendix A: 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/ vice 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.
- 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 electronically.
 - 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 will be stored electronically.
- The DPO and headteacher will meet to review what happened and how it can be prevented 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 above to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly high risk or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Appendix B: Parental Data Review Request Form

Data Review Request Form

Child's Details	
Child's Name	
Child's Date of Birth	
Child's Current Address	
Child's Current Class	
Person Requesting Data Review	
Your Name	
Your Relationship To the Child	
Your Address	
Your Telephone Number	
Do You Have Parental Responsibility ?	
Your Request	
What Data / Which Records Do You Wish To View ?	
Why Do You Wish To View Them ?	
What Do You Expect To Find In These Records ?	

Please sign this request

Signed :

Date :

Once completed, please hand this form into the school office who will ensure that it is forwarded to the right person (the school's Data Protection officer). You will be issued with a receipt for it. We are required to respond to your request within one calendar month of this request being received.

NB : Should your request be accepted, we would not normally make a charge. However, we reserve the legal right to do so if your request is vexatious, excessive or unfounded

Appendix C : Parental Data Amendment Request Form

Data Amendment Request Form

Child's Details	
Child's Name	
Child's Date of Birth	
Child's Current Address	
Child's Current Class	
Person Requesting Data Amendment	
Your Name	
Your Relationship To the Child	
Your Address	
Your Telephone Number	
Do You Have Parental Responsibility ?	
Your Request	
What Data / Which Records Do You Wish To Have Amended ?	
What Amendment Do You Want ? Do You Want It Updating, Amending Or Deleting ?	
Why Do You Want These Changes Undertaking ?	

Please sign this request

Signed :

Date :

Once completed, please hand this form into the school office who will ensure that it is forwarded to the right person (the school's Data Protection officer). You will be issued with a receipt for it. We are required to respond to your request within one calendar month of this request being received.

NB : Should your request be accepted, we would not normally make a charge. However, we reserve the legal right to do so if your request is vexatious, excessive or unfounded.

D: Retention of Data Protection Information

Data Subject	Document Name/ Type of Data	Reason for holding the data	Third Party Recipients	Retention Period	Paper/ electronic	Who has access	Method of destruction
Admin	Visitors book/ Entrysign electronic signing in system	Recording and monitoring visitors to school	None	current + 6 years	P&E	Office Staff, Headteacher	Electronic copy deleted and paper copy shredded at the end of the period of retention
Admissions	Admission Appeals	Legal requirement, pupil welfare	Independent appeals panel	Date of appeal +1 year	P&E	Headteacher, Business Manager, Governors Admission Committee	Electronic copy deleted and paper copy shredded at the end of the period of retention
Admissions	Supplementary Information Form	Required to support application process	None	If admitted - add to pupil record Unsuccessful - Date of application + 1 Year	P&E	Business Manager, Governors Admission Committee, Headteacher	Computer retains copy of records in 'Archive', paper copy shredded
Community Records	Community invitation list	Invitation to events	None	Current attendees only	E	Business Manager, Admin Assistant	Electronic record deleted when no longer current
Governors	Governor Personal Details	Legal requirement, safeguarding records	Oldham Council Governor Support, DfE website	End of term of office +1 year	P&E	Headteacher, Business Manager Chair of Governors	Electronic copy deleted and paper copy shredded at the end of the period of retention
Governors	Governors Emails	Held by individual governors for school improvement and pupil welfare	None unless legally required to share by request	Date of meeting	E	Governors/Sub Committee members	Electronic copy deleted at end of the meeting
Governors	Governor Minutes, principal signed	Legal requirement, school improvement	Oldham Council Governor Support	Permanent	P	Held by Oldham Council Governor Support	Retain permanently
Governors	Governor's minutes inspection copies & reports	School improvement and pupil welfare	Oldham Council Governor Support	Date of meeting + 6 years	P&E	Governors, Headteacher, Oldham Council Governor Support	Electronic copy deleted and paper copy shredded at the end of the period of retention
Governors	Complaints documentation	Legal requirement	None	Minimum - date of resolution +6 years.	P&E	Governor Complaints	Electronic copy deleted and paper copy shredded at the end

				Review contentious disputes before destroying		Committee, Headteacher	of the period of retention
Data Subject	Document Name/ Type of Data	Reason for holding the data	Third Party Recipients	Retention Period	Paper/ electronic	Who has access	Method of destruction
Governors/ Headteacher appraisal	Headteacher Appraisal documentation	School improvement, Personal and professional development	External Consultant appointed to Headteacher Appraisal by Governors	Current +5 years	P&E	Governors appraisal committee, Headteacher, SIP	Electronic copy deleted and paper copy shredded at the end of the period of retention
Health & Safety	Health & Safety Adult Accident AIRS forms	Legal requirement, staff and visitor welfare	Oldham Council Health & Safety where appropriate	Date of incident + 6 years	P&E	Headteacher/Staff /LA	Electronic copy deleted and paper copy shredded at the end of the period of retention
Health & Safety	Health & Safety Child Accident AIRS forms	Legal requirement, pupil welfare	Oldham Council Health & Safety where appropriate	dob + 25 years	P&E	Headteacher/Staff /LA	Electronic copy deleted and paper copy shredded at the end of the period of retention
Health & Safety	Health & Safety Policy and Risk Assessments	Legal requirement, welfare of staff, pupils & visitors	None	Current + 3 years	P&E	Headteacher, Governors, Staff, LA	Electronic copy deleted and paper copy shredded at the end of the period of retention
Health & Safety	Critical Incident Plan	Pupil and staff welfare and safety	Emergency services, HSE if required	Current	P&E	Headteacher, Deputy Head, Business Manager, Chair of Governors	Electronic copy deleted and paper shredded when new document produced.
Management	Records created by any management staff & Headteacher	Pupil monitoring and welfare	None	Date + 6 years	P&E	Headteacher/DHT /LMF/SLT	Electronic copy deleted and paper copy shredded at the end of the period of retention
Management	Headteacher reports, SLT & LMF minutes	School Management and improvement	None	Date of meeting + 3 Years	P&E	Headteacher/DHT /LMF/SLT	Electronic copy deleted and paper copy shredded at the end of the period of retention
Management	School Census	Legal requirement	DfE, Oldham Council	Current + 5 years	P&E	Headteacher, Business Manager	Electronic copy deleted and paper copy shredded at the end of the period of retention
Personnel	Staff Interview/	Legal requirement	None	Successful - whilst in	P&E	Headteacher,	Electronic copy deleted and

	Recruitment records & DBS			employment + 6 years Unsuccessful date of interview +6 months		Governors, L A, Diocese, Business Manager	paper copy shredded at the end of the period of retention
Personnel	Staff files	Legal requirement	Oldham Council HR where appropriate	Termination +6 years	P&E	Headteacher, Business Manager	Computer retains copy of basic records in 'Archive', paper copy shredded
Data Subject	Document Name/ Type of Data	Reason for holding the data	Third Party Recipients	Retention Period	Paper/ electronic	Who has access	Method of destruction
Personnel	Staff emergency contact details	Staff welfare	None	Termination	P&E	Headteacher, Business Manager	Electronic copy deleted and paper copy shredded at the end of the period of retention
Personnel	Staff annual appraisal	Staff personal and professional development	None	Current +5 Years	P&E	Headteacher, Deputy Head	Electronic copy deleted and paper copy shredded at the end of the period of retention
Personnel	Lesson Observations	School improvement, Staff personal and professional development	None	Current +5years	P&E	Headteacher, Deputy Head	Electronic copy deleted and paper copy shredded at the end of the period of retention
Personnel	Staff Disciplinary Records	Staff appraisal	Oldham HR as appropriate	Oral - date of warning + 6 months/Written level 1 date + 6months/ Written level 2 date +12 months/Final date of warning +18 months Dismissal	P&E	Headteacher	Electronic copy deleted at end of retention period
Personnel	Staff disciplinary of a safeguarding nature	Legal requirement, pupil welfare	Local Authority Safeguarding Officer	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then review. Allegations found to be malicious will be removed from the personnel files. If found they are to be	P&E	Headteacher	Electronic copy deleted and paper copy shredded at the end of the period of retention

				kept on file and a copy provided to the person concerned			
Property	School Lettings	Property management and financial records	None	Current + 6 years	P&E	Headteacher, Business Manager, Admin Assistant	Electronic copy deleted and paper copy shredded at the end of the period of retention
Data Subject	Document Name/ Type of Data	Reason for holding the data	Third Party Recipients	Retention Period	Paper/ electronic	Who has access	Method of destruction
Pupil	Pupil Correspondence to HT/DHT	Pupil welfare	None	Retain whilst pupil at school	P&E	Headteacher, Deputy Headteacher	Electronic copy deleted and paper copy shredded when pupil leaves the school
Pupil	Behaviour records/Reflection sheets	Pupil welfare	None	Until pupil leaves the school	P	Headteacher, teacher	Paper copy shredded when the pupil leaves the school
Pupil	Exclusion fixed or permanent	Legal requirement, pupil welfare	Oldham Council Pupil Welfare	Until pupil leaves the school	E	Headteacher	Electronic record deleted when no longer current, transfer to secondary school
Pupils	Pupil Annual Report	Pupil progress reporting to parents	None	Until pupil leaves the school	P&E	Teaching Staff, Business Manager	Until pupil leaves the school
Pupils	SEN File	Legal requirement, pupil welfare	Medical professionals as appropriate, transferred to next school	DOB +25	P&E	Headteacher, SENCo,	Paper copy transferred to next school. Paper copy also retained in school to end of retention period. Electronic copy deleted when child leaves the school.
Pupils	SATs results and papers	Legal requirement	DfE, Oldham Council	Current + 6 Years	P&E	Headteacher, Year 6 Teacher, Business Manager	Computer retains copy of records in 'Archive', paper copy shredded
Pupils	RAISE Online/ Aspire	pupil progress monitoring	DfE, Oldham Council	Current +6 years	P&E	Headteacher/ Deputy Head/ Governors	Electronic copy deleted and paper copy shredded at the end of the period of retention
Pupils	Internal assessment data	Pupil progress monitoring	None	Until pupil leaves the school, transfer to next school	P&E	Headteacher, Teaching Staff, Business Manager	Computer retains copy of records in 'Archive', paper copy shredded, data transferred to next school

Pupils	Medical Records	Pupil welfare	Medical professionals as appropriate	Until pupil leaves the school	P&E	Staff	Computer retains copy of records in 'Archive', paper copy shredded
Pupils	Parental Consent for school trip – No incident	Legal requirement, pupil welfare	None	Conclusion of trip	P&E	Headteacher, Staff, Admin Assistant	Electronic copy deleted and paper copy shredded at the end of trip
Pupils	Parental Consent for school trip - Major incident	Legal requirement, pupil welfare	Oldham Council Health & Safety, HSE	DOB of pupil +25 years, also retain consent forms for other pupils on trip	P&E	Headteacher, Staff, Admin Assistant	Electronic copy deleted and paper copy shredded at the end of the period of retention
Data Subject	Document Name/ Type of Data	Reason for holding the data	Third Party Recipients	Retention Period	Paper/ electronic	Who has access	Method of destruction
Pupils	Pupil File	Legal requirement, pupil welfare	Transferred to next school, DfE	Until child leaves the school	P&E	All staff	Computer retains copy of records in 'Archive', paper copy shredded
Pupils	Attendance registers	Legal requirement, pupil welfare	Oldham Council School Attendance, DfE	Until child leaves the school	P&E	Headteacher, Teachers, Business Manager, Admin Assistant	Computer retains copy of records in 'Archive', paper copy shredded
Pupils	Attendance/ absence letters/ penalty notice	Legal requirement, pupil welfare	Oldham Council School Attendance, DfE	Current + 2 years	P	Staff, Headteacher	Paper copy shredded at end of retention period
Pupils	Dinner Register including free school meal info	Catering management and financial records	ParentPay Ltd	Current + 6 Years	E	Headteacher, Admin Assistant, Business Manager	Free school meal eligibility - computer retains copy in archive Dinner register held on Parent pay until pupil leaves the school
Safeguarding	Single Central Record	Legal requirement, pupil welfare	Ofsted inspectors	Current only	P&E	Headteacher, Business Manager, Admin Assistant	Electronic entry deleted and paper copy shredded when no longer current
Safeguarding	Safeguarding file CPOMS	Legal requirement, pupil welfare	Next School where appropriate	DOB + 25 years	P&E	Headteacher	Electronic/Paper copy transferred to next school. Paper copy also retained in school to end of retention period. Electronic copy deleted when child leaves the school.

