



Moordown St John's CE Primary School

Policy for Data Protection

**"A Christian community where commitment to
educational excellence changes lives"**

Date Approved by Chair of Directors: 21st March 2024

Review Date: March 2027

A copy of this policy in an alternative format, such as large print or different language,
may be provided on request from the school office.

MOORDOWN ST JOHN'S CE PRIMARY SCHOOL

DATA PROTECTION POLICY



Contents

1. Aims.....	3
2. Legislation and guidance	3
3. Definitions	3
4. The data controller	4
5. Roles and responsibilities	4
6. Data protection principles.....	5
7. Collecting personal data.....	5
8. Sharing personal data	6
9. Subject access requests and other rights of individuals	7
10. Parental requests to see the educational record	8
11. CCTV	8
12. Photographs and videos	8
13. Artificial Intelligence	9
14. Data protection by design and default	9
15. Data security and storage of records.....	10
16. Disposal of records	10
17. Personal data breaches	10
18. Training.....	11
19. Monitoring arrangements	11
20. Links with other policies	11
Appendix 1: Personal data breach procedure.....	12

1. Aims

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

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

2. Legislation and guidance

This policy meets the requirements of the:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)

[Data Protection Act 2018 \(DPA 2018\)](#)

It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#).

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ➤ Name (including initials) ➤ Identification number ➤ Location data ➤ Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ➤ Racial or ethnic origin ➤ Political opinions ➤ Religious or philosophical beliefs ➤ Trade union membership ➤ Genetics ➤ Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ➤ Health – physical or mental ➤ Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.

TERM	DEFINITION
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

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

The school is registered with the ICO and has paid its data protection fee 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 Board of Directors

The Board of Directors has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 School-based data protection lead and independent data protection officer

The school-based data protection lead (DPL), in conjunction with our data protection officer (DPO), is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

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

Our school-based Data Protection Lead, **Kerri Chant**, is the first point of contact for individuals whose data the school processes. **Kerri** can be contacted via our school office:

Telephone: 01202 527683 **Email** k.chant@st-johns.bournemouth.sch.uk

Our independent Data Protection Officer, Kim Bainton, is the first point of contact for the Information Commissioner's Office. Kim can be contacted at Kingsleigh Primary School, Hadow Road, Bournemouth BH10 5HT Telephone: 01202 528893
Email kim.bainton@kingsleighprimary.co.uk

The Data Protection Lead, in consultation with the Headteacher, acts as the representative of the Data Controller on a day-to-day basis.

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 DPL/DPO in the following circumstances:

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

6. Data protection principles

The UK GDPR is based on data protection principles that 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/carers 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/carers when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**

- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

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

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

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

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

7.2 Limitation, minimisation and accuracy

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

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

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

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

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

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

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. This includes:

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

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

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

If staff receive a subject access request in any form they must immediately forward it to the DPO.

9.2 Children and subject access requests

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

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

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

As an Academy, there is no automatic parental right of access to your child's educational record. The school may choose to provide this upon request, however the best interests of the child will always be considered. To request access to your child's educational record, please contact The Board of Directors, via our Data Protection Lead. If access is agreed, this information is usually provided free of charge.

11. CCTV

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

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

Any enquiries about the CCTV system should be directed to our Estate Manager c/o the School Office, Telephone: 01202 527683 Email msjoffice@st-johns.bournemouth.sch.uk

12. 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, unless all the relevant parents/carers have agreed to this.

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

- Within school premises - internal displays, notice-boards etc
- School newsletter (*which is posted to our website and social media page*)
- Outside of school by external agencies (*such organisations may use such images on their websites*)
- Online on our school website or social media pages

The school photographer visits at least twice a year and will take individual, sibling, class and/or year group images where parents/carers have given permission.

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 Safeguarding/Child Protection policy, Online Safety including Acceptable Use policy, staff induction handbooks and volunteer/placement guidance notes for more information on our use of photographs and videos.

Parents/carers are reminded that all photographs/filmed images taken at school events (eg school plays/sports events/concerts) are for personal use only and should not be uploaded to social media sites.

13. Artificial Intelligence

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

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

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

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 **UK**, 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 UK 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/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
- Staff members are reminded that passwords to access the school network/email must be changed every term. Passwords must be at least 10 characters long and contain at least 3 of the following: upper case letters, lower case letters, numbers and/or special characters.
- Children have simple passwords that stay with them throughout their time at our school. Their passwords enable them to access the Student Resources folder plus their own personal folders – no other data can be accessed. Their passwords also provide access to learning software.
- The use of USB/removable devices to store/transport personal data is prohibited. However, in extreme circumstances, when remote access is down, a USB/removable device may be brought into school if it is the only option. The office/technical team must be asked to virus check the device before transferring and/or opening documents. If any viruses were transmitted, the staff member bringing in the removable device would be liable and subject to the school's capability process
- Staff, pupils or directors who store personal information on their personal devices (eg school email) are expected to follow the same security procedures as for school-owned equipment (see our acceptable use policies/agreements)
- 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)

If staff access school emails on their personal device, the following security measures must be adhered to:

- The personal device should have a pin code, finger or thumb print or face recognition access
- If staff open attachments on their personal device they must clear the 'downloads' folder regularly.
- If the device is lost or stolen, the staff member must report this to the Network Manager who will enforce an immediate password change on the school account.
- Staff should know how to 'Erase all data' if the device is lost or stolen (if this feature is available). Alternatively, the staff member must advise the technical support team as soon as they are aware that the device is missing so that unauthorised access may be blocked.

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.

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. Personal data breaches

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

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

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

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

18. Training

All staff and directors 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 data protection lead, in conjunction with the data protection officer, is responsible for monitoring and reviewing this policy.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety including Acceptable Use
- Safeguarding and Child Protection policy
- Staff induction handbook
- Volunteer/Work Experience/placement guidance notes
- *Cyber Response Plan – new policy to be created*

21. Policy review

This policy was carefully considered and ratified by the Board of Directors at its meeting on 30 November 2023. This policy was further updated in April 2024 to reflect a change in the school-based Data Protection Lead. The amended policy was considered and ratified by the Board of Directors at its **meeting on 21st March 2024**

This policy will be reviewed on a 3 yearly basis, with the next review taking place during March 2027.

The review will be brought forward should earlier changes in protocol be recommended by the Information Commissioner's Office, the Government, the Department for Education or the Diocese.

Signed:



Chair, Board of Directors

Date: 21st March 2024

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member, director or data processor must immediately notify the school-based data protection lead (DPL) who will in turn notify the data protection officer (DPO). *The contact details for the DPL and DPO are shown in Section 5 of this policy.*
- The school-based data protection lead, in conjunction with the data protection officer, will investigate the report, and determine whether a breach has occurred. To decide, the DPL/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
- Staff and directors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.
- If a breach has occurred or it is considered to be likely that is the case, the DPL/DPO will alert the headteacher and the chair of directors.
- The DPL/DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPL/DPO with this where necessary, and the DPL/DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure).
- The DPL/DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen before and after the implementation of steps to mitigate the consequences.
- The DPL/DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's [self-assessment tool](#).
- The DPL/DPO will document the decisions (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 within the school's GDPR Data Breach Recording Log (*stored on the Admin area of the school's computer network*).
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page](#) of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned.
 - The name and contact details of the DPO.
 - A description of the likely consequences of the personal data breach.
 - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - A description, in clear and plain language, of the nature of the personal data breach.
 - 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 consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the school's GDPR Data Breach Recording Log which is stored on the Admin area of the school's computer network.

- The DPL/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
- The DPL/DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try to mitigate the impact of different types of data breach if they were to occur, 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.

Sensitive information being disclosed via email (including safeguarding records)

- All sensitive information being sent via email should be password protected and/or encrypted prior to sending. A telephone call should be made to the recipient to advise of the password.
- Extra care should be taken to ensure the message is sent to the correct recipient. If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the network Manager/external IT support provider to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Sensitive information being disclosed via the post (including safeguarding records)

- The name and address of the recipient must be confirmed prior to the information being posted
- The information should be enclosed in a robust envelope or double enveloped and marked 'Private and Confidential – to be opened by addressee only'.
- The school address should be stamped on the reverse of the envelope.
- Where appropriate the information should be sent via Special Delivery / Signed for or sent via a courier.

- When necessary the recipient should be advised the information is being sent and they should be asked to confirm its safe receipt.

Other types of breach could include:

Details of pupil premium interventions for named children being published on the school website

- The Network Manager is the only person permitted to upload information to the website.
- Staff members are to provide the Network Manager with the items to upload; she will check for Data Protection compliance prior to actioning.
- Each year, all staff to read, sign and return the Acceptable Use policy

Non-anonymised pupil exam results or staff pay information being shared with Directors

- The Clerk to the Directors is the link between the school and the Board.
- Staff members are to provide the Clerk with the items for sharing at Board meetings at least one week in advance. The Clerk will check for Data Protection compliance prior to circulating. If the data is not in a suitable format for circulating, the Clerk will return the information to the author for updating.
- HR and curriculum reports to the Board to be anonymised prior to sharing with the Board. Same process to be followed for accident/incident reporting.

The school's cashless payment provider being hacked and financial details stolen

- Staff to follow correct password protocols: use only strong passwords which are regularly changed, do not share passwords with anyone, keep passwords in a secure location etc
- School to maintain good cyber security ~ the Network Manager to regularly check that the school's ICT infrastructure is secure and is not open to misuse or malicious attack..
- The Network Manager ensures the school meets the e-safety technical requirements outlined in the Online Safety including Acceptable Use policy and any 'best practice' from central government
- School's ICT support provider to make regular security checks of the school's ICT system/network.
- The School to carry out due diligence on all suppliers to ensure they are GDPR compliant and have the necessary technical and organisational infrastructure in place to minimise the risk of any breach.

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

- The Network Manager to ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- All staff to report any suspected misuse or problem to the Network Manager for investigation / action / sanction
- Laptops not to be left unattended in public (for example in cars or on public transport)
- All school laptops are accessed by strong passwords (see earlier point re password protocols)

A school memory stick/other portable device containing non-encrypted sensitive personal data being stolen or hacked

Use of USB memory sticks/removable devices to transport/hold personal information is forbidden except in extreme circumstances see *Section 15 of policy*.

Hard copies of reports being sent to the wrong pupils or families

- All reports sent via the post must be marked private and confidential, for addressee only and have the school address stamp on the reverse to enable safe return if the addressee has left the premises.
- A pupil update exercise will take place annually to check the accuracy of pupil contact data held.
- Parents/carers to be reminded at regular intervals of the importance of keeping the school updated of any changes to their contact information.

Staff training on Data Protection issues upon induction and at regular intervals thereafter should also minimise the risk of any data breaches.