



Alexandra Primary School Data Protection Policy

January 2020

Committee Responsible	
Status	Statutory
Reviewed	14/01/2020
Review Period	Bi-annual

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	6
8. Sharing personal data	6
9. Subject access requests and other rights of individuals	7
10. Parental requests to see the educational record	9
11. CCTV	10
12. Photographs and videos	10
13. Data protection by design and default	11
14. Data security and storage of records	11
15. Disposal of records	13
16. Personal data breaches	13
17. Training	13
18. Monitoring arrangements	13
19. Links with other policies	14
Appendix 1: Personal data breach procedure	14

1. Aims

Alexandra Primary aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018) and protects an individual's right to privacy.

The School will not exploit any imbalance in power in the relationship between the School and its data subjects.

The School is committed to ensuring that its staff are aware of data protection requirements and legal requirements and will raise awareness of the importance of compliance.

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](#)).

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 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 and also includes any expression of opinion about an individual, personal data held visually in photographs or video clips (including CCTV) or sound recordings.

.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.
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

This School collects and processes a large amount of personal data every year (relating to parents, pupils, staff, governors, visitors and others) including: staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data.

The School may also be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies (e.g. Department of Education) and other bodies.

To comply with the Data Protection legislation, this School will collect, use fairly, store safely and not disclose personal data to any other person unlawfully.

As our school processes personal data it is therefore a data controller and is registered as such with the ICO and will renew this registration annually or as otherwise legally required and will pay and required fees.

5. Roles and responsibilities

This policy applies to the school and **all staff** employed by our school, and to external organisations or individuals working on our behalf.. Data breaches can have serious effects on individuals and institutions concerned and can bring the School into disrepute. Members of the School community who breach this Policy and/or the Data Protection legislation will be subject to disciplinary action under the School's Disciplinary Policy, which can include sanctions up to and including dismissal. Such breaches may also lead to criminal prosecution.

5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations. Governors may periodically review the DPIAs to assess the School's compliance with the Data Protection legislation.

5.2 Data protection officer

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

- They will provide an annual report of their activities directly to the governing body and, where relevant, report to the Governing Body 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.

They will prepare and use Data Protection Impact Assessments (DPIA) to help assess and mitigate data privacy risks to children and in particular where the School processes data that is likely to result in a high risk to the rights and freedom of its pupils it will always complete a DPIA.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

<https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/>

<https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/>

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacy>

<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacy-impact-assessments-code-published/impact-assessments-code-published/>

Our DPO is Heidi Bennett and is contactable via e-mail at admin@alexprimary.haringey.sch.uk.

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 and in accordance with the GDPR and all relevant legislation. In particular but not exclusively
- All members of the school community are responsible for taking care when handling, using or transferring personal data.
- All members of the school community have a responsibility for ensuring that data cannot be accessed by anyone who does not have permission to access that data.
- 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 e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, 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 which are set out in the GDPR and Data Protection Act 2018.

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

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

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.

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 . (See Appendix 2).

We will keep data up to date and rectify any incorrect data

8. Sharing personal data

We will not normally share personal data with anyone else, but there may be certain circumstances when 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 however we may disclose data without consent in certain circumstances such as :

Other schools

If a pupil transfers from Alexandra Primary to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation, which should ensure that there is minimal impact on the child's academic progress because of the move.

Examination authorities This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and courts If a situation arises where a criminal investigation is being carried out, the School may have to forward information on to the police to aid their investigation. The School will pass information onto courts as and when it is ordered.

Social workers and support agencies In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational division The School may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

- o 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:
- o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- o Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

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

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- Where 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 safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form but may be responded to more quickly if made in writing, either by letter or email to the DPO. They should 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 within 1 month of receipt of the additional information requested to confirm identity)
- 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 which covers administrative costs.

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

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or that they can seek to enforce their subject access rights 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
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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. The School need not comply with a request for erasure or the restriction etc if it is holding and using the data for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

The School will design its processes so that, as far as possible, it is as easy for a data subject to have their personal data erased as it was for the individual to give their consent in the first place.

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.

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.

12. 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 Heidi Bennett, School Business Manager.

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.

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.

It is the school's policy that external parties (including parents) may not capture images of staff or pupils within the school or taken as part of educational activities

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 (or pupils where appropriate) have agreed to this.

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 privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the 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
- That appropriate safeguarding is in place if we transfer any personal data outside of the EEA where different data protection laws 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 safeguarding of 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, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded not to use 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

The School will use proportionate physical and technical measures to secure personal data.

The School will consider the security arrangements of any organisation with which data is shared shall and where require these organisations to provide evidence of the compliance with the DPA 2018 and GDPR.

The School will store hard copy data, records, and personal information out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will only be stored where it is necessary to ensure the safety of children and not kept on open display.

Sensitive or personal information and data should not be removed from the school site, however, the School acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

To reduce the risk of personal data being compromised any individual taking personal data away from the School site must adhere to the following:

- Paper copies of personal data should not be taken off the school site as if misplaced they are easily accessed. If no alternative is available other than to take paper copies of data off the school site then the individual must ensure that the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files must be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Individuals must take care to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- Where information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- Teaching Staff must ensure that personal data and sensitive personal data is not displayed inadvertently on White Boards during class lessons.
- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only. USB sticks that staff use must be password protected.
- Breaches of the policy will be dealt with in accordance with the School's disciplinary policy and could amount to gross misconduct.

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. Some data may be retained after employees or pupils have left the school

Examples, of appropriate disposal include shredding or incinerating paper-based records, and overwriting or deleting 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.

The creation of systems and/or files, which duplicate such data will be avoided; where it is inevitable every care will be taken to ensure that data maintained in secondary systems is accurate and kept up to date.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

Timescales for the retention of records will be in accordance with ICO guidance

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. 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.

This policy will be reviewed **every 2 years** and shared with the full governing board.

20. Links with other policies

This data protection policy is linked to our Freedom of information publication scheme

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 school's computer system.
- 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:
 - The name and contact details of the DPO
 - A description in clear and plain language of the nature of the personal data breach
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The decision on whether to contact individuals will be recorded 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 and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system.

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 take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- Sensitive information being disclosed via email (including safeguarding records)
 - If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
 - Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
 - If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website

Examples of other types of breach that could occur include you might want to consider could include:

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