Laycock Primary School



Data Protection Policy

Approved by Chair of IEB:	Prudence Barnes-Kemp
Ratified and reviewed on:	7th November 2025
Next review due by:	November 2026

Contents

1. Aims 3
2. Legislation and guidance 3
3. Definitions 3
4. The data controller 5
5. Roles and responsibilities 5
5.1 Governing board 5
5.2 Data protection officer 5
5.3 Representative of the data controller 5
5.4 All staff 5
6. The data protection principles 6
7. Processing personal data 6
7.1 Lawfulness, fairness and transparency 6
7.2 Limitation, minimisation and accuracy 7
8. Sharing personal data 8
9. Artificial intelligence (AI) 8
10. Transferring Data Internationally 9
11. Individuals Data Protection Rights 9
11.1 Access Rights 9
11.2 Other Rights regarding your Data: 9
11.3 Children and Data Rights/Request 11
12. Parental requests to see the educational record 11
13. Close Circuit Television (CCTV) 11
14. Photographs and videos 12
15. Data protection by design and default 12
16. Data security and storage of records 13
17. Disposable of records 13
18. Personal data breaches 13
19. Training 14
20. Monitoring arrangements 14
21. Links with other policies 14
Appendix 1: Date Breach Procedure 15

1. Aims

Our school aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a member of the school workforce, pupil/student, parent, Governor, visitors, contractor, consultant, or any other individual is done so in accordance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018), Data (Use and Access) Act (DUAA) 2025 and the Privacy & Electronic Communications (EC Directive) Regulations (PECR) 2011.

This policy applies to all personal data processed by the school, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

2. Legislation and guidance

This policy meets the current requirements of UK Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the EU GDPR, PECR 2011, UK GDPR, DUAA 2025 and DPA 2018. It is also based on the information provided by the Article 29 Working Party.

Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to video surveillance, and the DBS Code of Practice in relation to handling sensitive information. Furthermore, this policy complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

TERM	DEFINITION
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the Controller's instruction.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes via a statement or by a clear affirmative action, signifying agreement to a specific processing of personal data relating to them.

TERM	DEFINITION
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a › name, › an identification number, › location data, › an online identifier or › to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
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 › History of offences, convictions or cautions* * Note: Whilst criminal offences are not listed as special category data, within this policy they are regarded as such in acknowledgment of the extra care which is needed with this data set.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing can be automated or manual.
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

The School collects and determines the processing for personal data relating to parents/carers, pupils, the school workforce, governors/volunteers, visitors and others, in addition they process data on the behalf of others therefore are considered a data controller and a data processor.

The School is registered as a data controller with the ICO and will renew this registration as legally required, the registration number is **ZA216993**

5. Roles and responsibilities

This policy applies to **all individuals** employed by our school, and to external organisations or individuals working on our behalf. Employees who do not comply with this policy may face disciplinary action.

5.1 Governing board

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

5.2 Data protection officer

The School has appointed Grow Education Partners Ltd as its Data Protection Officer (DPO), the responsible contact is Claire Mehegan claire.mehegan@london.anglican.org

They are responsible for overseeing the implementation of this policy, along with any future development of this or related policies/guidelines and reviewing our compliance with data protection law.

Upon request the DPO can provide an annual report of the school's compliance status directly to the governing board and will report to the board their advice and recommendations on school data protection issues.

The DPO is a named point of contact for all Data Subjects whose data the school processes, and for the ICO. Full details of the DPO's responsibilities are set out in their Service Level Agreement.

5.3 Representative of the data controller

The School Business Manager, Burcu Melemez, acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Employees (regardless of role) 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, e.g., change of address, telephone number, or bank details.
- Reporting a Data Breach, Data Rights Request, or Freedom of Information Request.
- Contacting the Data Protection Lead or DPO:
    - 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/notification, or transfer personal data outside the United Kingdom.
- 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. The data protection principles

Data Protection is based on seven principles that the school must comply with.
These are 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

The Accountability principle ties these all together by requiring an organisation to take responsibility for complying with the other six principles. Including having appropriate measures and records in place to be able to demonstrate compliance.

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

7. Processing personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The individual (or their parent/carer when appropriate) has freely given clear **consent**
- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law.

These are where:

- The individual (or their parent/carer when appropriate in the case of a pupil) has **given explicit consent;**
- It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a Data Controller or of a Data Subject.
- It is necessary to protect the **vital interests** of the Data Subject;
- Processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.**
- The Personal Data has **manifestly been made public** by the Data Subject;
- There is the **establishment, exercise or defence of a legal claim**;
- There are reasons of **public interest** in the area of **public health**;
- Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment);
- There are **archiving** purposes in the **public interest**;

Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice.

These privacy notices can be found in on our website's data protection page and relevant to the data subjects

- Pupils and Parents/Carers https://www.laycock.islington.sch.uk/our-school/gdpr
- School Workforce (includes Trainees, Contractors and Consultants) https://www.laycock.islington.sch.uk/our-school/gdpr
- Governors & Volunteers https://www.laycock.islington.sch.uk/our-school/gdpr
- Job Applicants https://www.laycock.islington.sch.uk/our-school/gdpr
- Visitors https://www.laycock.islington.sch.uk/our-school/gdpr

Additional Copies of the Privacy Notices are available on request by contacting the school office.

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 via our privacy notices.

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.

Employees must only access and process personal data where it is necessary to do their jobs.

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

When personal data is longer required, employees must ensure it is destroyed. This will be done in accordance with the school data retention policy, which states how long particular documents should be kept, and how they should be destroyed.

Copies of the Data Retention Policy can be obtained by contacting the School Business Manager, Burcu Melemez.

8. Sharing personal data

In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but 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 may seek consent when appropriate before doing this where possible
- Our suppliers or contractors need data to enable us to provide services to our employees 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 and have satisfactory security measures in place.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies when required to do so, these include but are not limited to:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees.

9. Artificial intelligence (AI)

(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. The 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. The School will treat this as a data breach, and will follow the personal data breach procedure outlined in this policy

10. Transferring Data Internationally

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

11. Individuals Data Protection Rights

11.1 Access Rights

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.
If you make a subject access request, and if we do hold information about you, we can:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- NOT provide information where it compromises the privacy of others.
- Give you a copy of the information in an intelligible form.

11.2 Other Rights regarding your Data:

You may also

- Withdraw their consent to processing at any time, this only relates to tasks which the school relies on consent to process the data.
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of your personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.

- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Refer a complaint to the ICO
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, individuals are asked to preferably submit their request in written format to assist with comprehension.

They should include:

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

If you would like to exercise any of the rights or requests listed above, please contact Burcu Melemez

- Office@laycock.islington.sch.uk
- 0207 226 2927
- Laycock Primary School, Laycock Street, London N1 1SW

If an individual receives a requests, they must immediately forward it to the School Business Manager, Burcu Melemez.

We reserve the right to verify the requesters identification by asking for Photo ID, if this proves insufficient then further ID may be required.

In most cases, we will respond to requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

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

A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.
When responding to requests, we will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual; or

- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning the child

In the event we refuse a request, we will tell the individual why, and tell them they have the right to refer a complaint to the ICO.

Article 22 of the UK GDPR has additional rules to protect individuals from decisions made solely for the purpose of automated decision-making and profiling. The school does not carry out any automated decision-making and/or profiling on individuals.

11.3 Children and Data Rights/Request

An individual's data belongs to them therefore a child's data belongs to that child, and not the child's parents or carers.

However, children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, for children under the age of 12 most data 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.

Where a child is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, we would require them to give consent to authorise the action to be undertaken.

12. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. Requests should be made in writing to the *Contact details for Educational Record Requests* and should include;

- Name of individual making the request and child who the education record belongs to
- Requester's correspondence address
- Requesters contact number and email address

13. Close Circuit Television (CCTV)

We use CCTV in various locations around the school sites and premises for the detection and prevention of crime. However, footage may be used for additional reasons specified more fully in the CCTV Policy. We adhere to the ICO's code of practice for the use of video surveillance and provide training to staff in its use.

We do not need to ask individuals' permission to use CCTV, but in most instances, we make it clear where individuals are being recorded, with security cameras that are clearly visible and accompanied by prominent signs explaining that CCTV is in use, and where it is not clear, directions will be given on how further information can be sought.

The full CCTV policy can be found on our website. Any enquiries about the CCTV system should be directed to Burcu Melemez, School Business Manager.

14. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

The use of school photographs includes but is not limited to:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies and partners such as the school photographer, local and national newspapers and local and national campaigns we are involved with
- Online on our website or social media pages

We will obtain consent from the responsible individuals to use pupil images. When doing so we will clearly explain how the photograph and/or video will be collected and used to both the parent/carer and pupil when obtaining consent.

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.

You can withdraw consent by informing the school office by email or in person.

See our Safeguarding and Child Protection Policy for more information on our use of photographs and videos. This can be found https://www.laycock.islington.sch.uk/our-school/safeguarding

15. 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 collection and processing activities. These include, but are not limited to the following organisational and technical measures:

- 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 regulations.
- Completing data 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 or processing tools. Advice and guidance will be sought from the DPO.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Periodic audits will be undertaken to monitor and review 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

16. 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.
Our organisational and technical measures include, but are not limited to;

- Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data will be kept under lock and key when not in use. We endorse a clear desk policy.
- Papers containing confidential personal data will not be left out on display when not in use unless there is a compelling lawful basis to do so e.g. Public Task to display Allergy information in the Medical Room.
- Passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Those who utilise school-controlled devices or platforms are reminded to change their passwords at regular intervals.
- Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.
- Employees, Pupils or Governors/Volunteers who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see School's Online & E- safety policy)
- 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.

17. Disposable 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 be rectified or updated, unless it is no longer of use and therefore will be disposed of securely.

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 and provide a certificate of destruction.

When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

18. Personal data breaches

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

All potential or confirmed Data Breach incidents should be reported to the School Business Manager, Burcu Melemez where they will be assigned a unique refence number and recorded in the school's data breach log.

Once logged, incidents will then be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.

Where appropriate, we will report the data breach to the ICO and affected Data Subjects within 72 hours. The full procedure is set out in the School Breach Procedure, Appendix 1

Examples of a Data Protection Breach include but are not limited to:

- Personal data being let unattended in a meeting room/in the staffroom/in the PPA room.
- Sending information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent
- 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

19. Training

All employees and governors are provided with data protection training as part of their induction process.

Periodic refresher will be provided to adhere to ICO best practice or to respond to changes in legislation, guidance or the school's processes. Records of attendance will be kept ensuring that all data handlers receive appropriate training.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work, they carry out.

They will work with the School's Data Protection Lead, Burcu Melemez and the Lead Governor for Data Protection to ensure that this policy remains contemporaneous and appropriate.

This policy will be reviewed yearly, and changes recommended when appropriate. The Governors will be asked to sign off the policy review and any necessary changes.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information Policy (publication scheme)
- Online and E-safety policy
- Acceptable Use Policy (AUP)
- Data Retention Policy and Schedule
- Staff Code of Conduct
- Safeguarding and child protection policy
- CCTV Policy

Appendix 1: Date Breach Procedure

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

Breach Notification

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the School Business Manager, Burcu Melemez, 0207 226 2927

They will make a decision whether to refer the matter to the Data Protection Officer (DPO) Claire Mehegan, claire.mehegan@london.anglican.org

Irrespective of whether the DPO is notified or not the response to the breach will follow the same path and be broken down into four distinct sections: **Investigation, Recovery, Reporting, Remedial Action.**

Investigation, Recovery and Reporting must be undertaken within 72hrs of breach realization. Remedial Action must be considered and decided on within this time frame but does not need to be fully enacted. 72hrs is the period of time which Data Protection Act 2018 allows for referral to the ICO or Data subjects.

Stage 1: Investigation:

All suspected breaches will be entered onto the "Data Breach Log" and assigned a unique reference number. All subsequent information will then be recorded on this log.

In addition, where required a corresponding file should be opened named after the unique reference number. All articles relating to the investigation, recovery and reporting should be stored within this file.

The first stages of the investigation into the breach report is to determine whether a breach has occurred by deciding if personal data has been accidentally or unlawfully mishandled. This will be done by assessing whether the data has been:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorized people

If a breach has been confirmed, then the severity of it will be assessed by considering:

- Data subject affected (vulnerability)Number of Data subjects affected.
- Data type lost, personal identifying/ special category,
- Specific Data Sets lost
- Number of Data sets
- Format of Data, electronic/paper.

Stage 2 Recovery:

The next stage is to contain and minimize the impact of the breach, this will be assisted by relevant staff members or data processors where necessary.

This may include but not be limited to:

- Contacting parties who may have received the data.
- Email Recovery
- Backup file restoration
- Requesting deletion of data.

If the data has been sent to the wrong individual and it has been requested to be deleted, confirmation of deletion should be attained in a written format for posterity.

The success or failure of the recovery must be recorded and will inform the reporting stage.

Stage 3: Remedial Action.

Once the detail of the breach is known and as the recovery process is being undertaken an assessment needs to be made on what potential future action could be considered to prevent a similar breach reoccurring.

This will involve reviewing the processes and procedures which may have failed resulting in the breach.

Potential remedial actions may include, but are not limited to:

- Anonymizing and minimizing data
- Encrypted drives
- Secure access servers
- Strong password setting
- Training and support for staff and governors
- Encrypted email

All potential remedial action is to be recorded on the Data Log.

Stage 4 Reporting:

The investigator must decide who should be informed about the breach, affected data subjects and/or the ICO

- Depending on the result of the containment efforts, the investigator will review the potential consequences, assess their seriousness and likelihood then make a decision about who needs to be informed. This will be partly determined by assessing if the risk of damage caused by the breach exceeds that of the damage that may be caused to the relationship through being informed.

If the risk of personal damage exceeds that of relationship, the Data Subjects will be promptly informed, in writing, all individuals whose personal data has been breached. This notification will set out:

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

The decision on whether to contact individuals will be documented.

A decision also needs to be made if the breach has reached the threshold to be reported to the ICO. This must be judged on a case-by-case basis.

To decide, the investigator 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
- Unauthorized reversal of pseudonymization (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 decision will be documented 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 *Place Decisions are documented*

- Where the ICO must be notified, this will be done 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 all known details of the breach including recovery attempts and their success. Potential remedial action will be included if known.

If all the breach details are not yet known, then as much as is known should be reported to the ICO within 72 hours. The report will explain that there is a delay, the reasons why, and when the further information is expected to be known. Then the remaining information will be submitted as soon as possible

At the conclusion of all stages of the Data Breach a mini report can be supplied to the Headteacher and Governors to brief them the outcome and propose ways it can be prevented from occurring again.

This is to allow Governors to hold the school accountable as per the Accountability Principle.

What is a personal data breach and what must staff do about them?

Some examples:

- I have been sent another staff member's pay slip
- I have been copied into an email about a pupil I don't teach or work with
- I have been sent data about another member of staff in the school or a pupil I don't teach
- I found sensitive personal data left in a meeting room/in the staffroom/in the PPA room
- I have sent information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent. (Whoops, pesky autofill!)
- I sent sensitive data/documents without either encryption or password protection, to the wrong person by accident
- I have lost something at home, but I am pretty sure it is there…
- I put something into the wrong envelope to the wrong person in the school
- I put something into the wrong envelope to the wrong parent
- I lost a memory stick
- I sent work emails to staff personal email accounts or from personal email accounts
- I had a break-in at home and my school laptop was stolen
- I took a set of books home to mark but accidentally left them on the bus
- I accidentally deleted a document containing personal data on the shared drive… and there's no back-up

What to do when a breach is spotted:

Low-level data breaches should be rectified, as far as possible, and added to the school's personal data breach log (in the same way you would log a playground accident where a pupil scrapes their knee and needs a plaster in the accident book).

Serious data breaches 'likely to have a significant detrimental effect' on data subject(s) – i.e. the people whose data has been lost/inappropriately viewed/stolen etc - need to be reported to the ICO within 72 hours of anyone at the school becoming aware of them. If there is a 'high risk' to data subject's rights and freedoms, the data subjects must also be notified.

All incidents should be recorded in the school's breach log. If you're in any doubt as to whether the ICO or data subjects should be notified, speak to your school Data Protection Lead (usually a member of SLT) or contact your Data Protection Officer.