Haggerston School

Aspiration Creativity Character

Data Protection Policy

Approved by	Date:
Full Governing Body	**3rd July 2023**
Monitored by:	**Full Review Due:**
School Business Leader	July 2024

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with 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 GDPR.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance 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.
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 are regarded as such in acknowledgement of the extra care which is needed with this data set.*
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

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

The school is registered with the ICO, and will renew this registration as legally required. The registration number is Z857458.

5. Roles and responsibilities

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

5.1 Governing Body

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

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 reports of their activities directly to the governing board and, where relevant, present to the board their advice and recommendations on school data protection issues.

The DPO is a named 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.

We have appointed Grow Partners Ltd as the Data Protection Officer (DPO). They are contactable by post: London Diocesan Board for Schools, London Diocesan House, 36 Causton Street, London, SW1P 4AU. By Phone: 020 7932 1100, by email schoolsDPO@london.anglican.org.

In addition to our outsourced DPO, we have a staff member who manages data protection day to day. The Data Protection Lead in our School is Ilias Avramidis, School Business Leader.
(Address: Haggerston School, Weymouth Terrace, London E2 8LS / Tel: 020 7739 7324 / email: subject.access@haggerston.hackney.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
- Informing the school of any changes to their personal data, such as a change of address
- Reporting a Data Breach, Data Right Request, or Freedom of Information Request.
- 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/notification, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - 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 seven 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

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 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual

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

Whenever we first 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 a location accessible and relevant to the data subjects:

- Pupils and Parents/Carers: School Website https://haggerston.hackney.sch.uk/wp-content/uploads/2021/04/HAG-Privacy-Notice-for-Students-Parents-Carers-23-Apr-2021.pdf
- School Workforce (includes Trainees, Contractors and Consultants): School Website

  https://haggerston.hackney.sch.uk/wp-content/uploads/2021/04/HAG-Privacy-Notice-for-School-Workforce-23-Apr-2021.pdf
- Governors & Volunteers: *School Website*

  https://haggerston.hackney.sch.uk/wp-content/uploads/2021/04/HAG-Privacy-Notice-for-GovernorsVolunteers-23-Apr-2021.pdf
- Job Applicants: School Website https://haggerston.hackney.sch.uk/wp-content/uploads/2021/04/HAG-Privacy-Notice-for-Applicants-23-Apr-2021.pdf
- Visitors: School Website

  https://haggerston.hackney.sch.uk/wp-content/uploads/2021/04/HAG-Privacy-Notice-for-Visitors-23-Apr-2021.pdf

Additional Copies of the Privacy Notices are available on request by contacting subject.access@haggerston.hackney.sch.uk

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.

Employees 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.

Copies of the Document Retention Policy can be obtained by contacting:
subject.access@haggerston.hackney.sch.uk

8. Sharing personal data
8.1 Sharing information and 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 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 UK 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.

8.2 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.

From 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.

9. Individuals Data Protection Rights

9.1 Access Requests

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 will:

- 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.

9.2 Other Rights regarding your Data

- 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 their personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of their 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 their personal data is transferred outside of the UK
- 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
- Submit 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)

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.

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

If you would like to exercise any of the rights or requests listed above, please contact The Data Protection Lead in our School, who is Ilias Avramidis, School Business Leader.
(Address: Haggerston School, Weymouth Terrace, London E2 8LS / Tel: 020 7739 7324 / email: subject.access@haggerston.hackney.sch.uk).

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 staff receive a subject access request, they must immediately forward it to the school Data Protection Lead.

9.3 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 aged 12 and above are generally 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 not 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.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site and premises to ensure it remains safe. However, footage may be used for additional reasons specified more fully in the CCTV Policy.We will adhere to the ICO's guidance on video surveillance.

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 the School Business Leader (subject.access@haggerston.hackney.sch.uk).

The full CCTV policy is available upon request.

13. Photographs and videos

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

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

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

We will obtain consent from the responsible individuals to use photos and images for communication, marketing and promotional materials. 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 writing to the Student & Data Services Team: student.dataservices@haggerston.hackney.sch.uk

When using photographs and videos we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Safeguarding policy for more information on our use of photographs and videos.

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, 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 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, 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, how and why we are storing the data, 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 our organisational and technical measures include but are not limited to:

- 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 staff room table, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

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.

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

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.

All potential or confirmed Data Breach incidents should be reported to the Data Protection Lead, who is the School Business Leader. (Address: Haggerston School, Weymouth Terrace, London E2 8LS / Tel: 020 7739 7324 / email: subject.access@haggerston.hackney.sch.uk).

Where they will be assigned a unique reference 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 Management Policy, which is available upon request. Examples of a Data Protection Breach 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 will be provided with data protection training.

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 annually and approved by the full governing board.

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information Policy
- CCTV Policy

APPENDIX 1: Data Breach Procedures

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 Data Protection Lead, who is the School Business Leader.*
(Address: Haggerston School, Weymouth Terrace, London E2 8LS / Tel: 020 7739 7324 / email: subject.access@haggerston.hackney.sch.uk).

They will make a decision where to refer the matter to the Data Protection Officer (DPO). (Grow Partners Ltd, London Diocesan Board for Schools, London Diocesan House, 36 Causton Street, London, SW1P 4AU / Tel: 020 7932 1100 / email: schoolsDPO@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 realisation. This is the period of time which Data Protection 2018 allows for referral to the ICO or Data subjects.

Stage 1: Investigation:
Investigation into the breach report 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 unauthorised people

Once 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.

Once a breach has been confirmed, it 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, a requisite 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.

Stage 2 Recovery:

Next stage is to contain and minimise 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 action of the next stage.

Stage 3 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.

  If the risk of damage is high, 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.

1) 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 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 in the school's shared drive.

- 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:

- If all the above 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 further information is expected to be known. Then the remaining information will be submitted as soon as possible

Stage 4: Remedial Action.

Finally, the breach will be assessed, and potential future actions considered on how to prevent a similar breach reoccurring.

Such actions include, but are not limited to:

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

At the conclusion of all stages of the Data Breach a mini report can be supplied to the Headteacher and Governors to brief them on 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 GDPR Principle of accountability.