Data Protection Policy & Procedure

This policy applies to all pupils and staff of Abbot's Hill, including EYFS.

In this policy reference to pupils includes past as well as present pupils.

1. Introduction

1.1 Abbot's Hill 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 the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

2. Legislation and guidance

2.1 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 meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

2.2 The school's reference number is Z5766966.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin

	• Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
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

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

4.2 The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

6. Governors

6.1 The Board of Governors has overall responsibility for ensuring that our school complies with all relevant data protection obligations and delegates the day to day responsibility for this to the Head and Bursar.

7. Data Protection Officer, Data Protection Lead and Data Compliance Officer

7.1 The school has chosen not to appoint a Data Protection Officer (DPO). There is no legal requirement to appoint one in an independent school.

7.2 The Bursar is the Data Protection Lead (DPL) for the school and is the first point of contact for any queries regarding data protection.

7.3 The ICT Network Manager is the Data Compliance Officer (DCO) and is responsible for monitoring our compliance with data protection law and developing related policies and guidelines where applicable.

8. All staff

8.1 Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPL 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

9. Data protection principles

9.1 The GDPR is based on data protection principles that our school must comply with.

9.2 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

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

10. Collecting personal data

Lawfulness, fairness and transparency

10.1 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 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)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

10.2 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.

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

Limitation, minimisation and accuracy

10.4 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.

10.5 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.

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

10.7 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 Data Retention Policy.

11. Sharing personal data

11.1 We will not normally share personal data with anyone else, but may do so where:

- We need to give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend
- We need to give information relating to outstanding fees or payment history to any educational institution which it is proposed the pupil may attend
- We need to publish the results of public examinations or other achievements of pupils of the school
- We need to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for instance to get accurate medical advice

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to pass information relating to outstanding fees onto a debt collection agency
- We need to liaise with other agencies – we will seek consent as necessary before doing this as long as this does not put the pupil at further risk
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a 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

11.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- 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

11.3 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.

11.4 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.

12. Subject access requests and other rights of individuals

Subject access requests

12.1 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 is not 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

12.2 Subject access requests must be submitted in writing, either by letter or email to the DPL.

12.3 They should include:

- Name of individual

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

12.4 If staff receive a subject access request they must immediately forward it to the DPL.

Children and subject access requests

12.5 Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian 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.

12.6 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 guardians 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.

12.7 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.

Responding to subject access requests

12.8 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
- 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

12.9 We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- 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
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

12.10 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account 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.

Other data protection rights of the individual

12.11 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 above), 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, or object to the processing of it (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)

12.2 Individuals should submit any request to exercise these rights to the DPL. If staff receive such a request, they must immediately forward it to the DPL.

13. Parental requests to see the educational record

13.1 There is no automatic parental right of access to their child's educational record in an independent school. The school is not required to disclose any pupil examination scripts. For further information, please see the Public Examinations Policy.

14. Biometric recognition systems

14.1 The Nursery has a biometric entry system. Parents/guardians have the right to choose not to use this system. We will provide alternative means of accessing the relevant services for those parents/guardians.

14.2 Parents/guardians can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

14.3 Where staff members or other adults use the school's biometric system, 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.

15. CCTV

15.1 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.

15.2 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.

15.3 Any enquiries about the CCTV system should be directed to the Bursar.

16. Photographs and videos

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

16.2 We will obtain written consent where necessary from parents/guardians for photographs and videos in accordance with our Image Authorisation Policy.

16.3 Where we need parental consent, we will clearly explain how the photographs and/or videos will be used to both the parent/guardian and pupil. Where we do not need parental consent, we will clearly explain to the pupil how the photographs and/or videos will be used.

16.4 Uses may include: school publications including the prospectus, magazine, brochures, the school website and e-newsletter and school social media sites, including Facebook and Twitter. External agencies may also take photographs including the school photographers, newspapers and/or advertising campaigns. Consent can be refused or withdrawn at any time. See our Image Authorisation Policy for more information on our use of photographs and videos.

17. Alumni and former staff members

17.1 We will obtain written consent from pupils/former pupils/former members of staff in order to maintain relationships with them once they have left the school for information, invitations to school events, marketing, fundraising or promotional purposes. This may include transferring information to any association, club or society set up for the purposes described above.

18. Data protection by design and default

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

- Appointing suitably trained staff, 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
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test 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 DPL and all information we are required to share about how we use and process their personal data (via our Privacy Notice)

- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

19. Data security and storage of records

19.1 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.

19.2 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 for a school trip, staff must agree with the Educational Visits Co-ordinator (EVC) which information can be taken and ensure that it is destroyed at the end of the trip in line with the Educational Visits Policy. All medical information (both for trips and sports matches) should be obtained from the School Nurse and must be returned to the School Nurse as soon as the trip/match is over. This includes copies given to other members of staff. Any other data must be destroyed safely or filed securely at the end of each visit.
- Passwords for staff are required to contain at least 8 characters including letters, numbers and symbols (ICT staff are required to have longer passwords). These are used to access school computers and other relevant devices. Staff and pupils are required to change their passwords at regular intervals
- Encryption software is not currently used but is being considered in order to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors accessing school data on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Online 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.

20. Disposal of records

20.1 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.

20.2 For example, we will confidentially 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.

20.3 Safeguarding records may be kept if the school is advised to do so.

21. Personal data breaches

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

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

21.3 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
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

22. Training

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

22.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

23. Monitoring arrangements

23.1 The Head and Bursar are responsible for monitoring and reviewing this policy.

23.2 This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing body.

Signed
Issue Date: May 2018
Review Date: May 2020 or earlier if major change requires

Mrs Kathryn Gorman
Head

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 DPL
- The DPL will investigate the report, and determine whether a breach has occurred. To decide, the DPL 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 DPL will alert the Head and the Chair of Governors
- The DPL 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 DPL will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPL 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 DPL 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 is likely that there will be a risk to people's rights and freedoms, the DPL will notify the ICO.
- The DPL 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 electronic filing system.
- Where the ICO must be notified, the DPL will do this via the 'report a breach' page of the ICO website within 72 hours. The DPL 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 DPL
    - 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 DPL 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 DPL expects to have further information. The DPL will submit the remaining information as soon as possible

- The DPL 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 DPL 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 DPL
    - 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 DPL 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 DPL 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 electronic filing system
- The DPL and Head 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)

- Safeguarding records must never be sent electronically unless using a programme such as CPOMS. If information is sent in error the following steps are also taken.
- 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, the Head and the DPL as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Head or DPL will ask the ICT department to recall it
- In any cases where the recall is unsuccessful, the Head or DPL 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 Head or DPL will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPL will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted