DATA PROTECTION POLICY

This policy applies to EYFS as well as whole school

Owner	Bursar
Authorised by	Head, Bursar and Governors
Dated	May 2020
Review	May 2021

Contents

1. Aims

Our school aim 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 Data Protection Act 2018 encompassing the General Data Protection Regulation (GDPR). 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 DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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 as defined by DPA2018	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 – N/A at DHS • 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

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

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

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 board

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

5.2 Data protection officer

As a small, independent school, we are not required to and do not have a dedicated data protection officer. The Bursar and the Head have joint responsibility for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

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

The Bursar is the first point of contact for individuals whose data the school processes and for the ICO.

Full details of the Head and the Bursar's responsibilities are set out in their job descriptions.

Our Bursar, as first point of contact, is contactable via email: mmitchell@derbyhigh.derby.sch.uk

5.3 Headteacher

The Head acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

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

6. Data protection principles

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

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed – see our Data Retention Policy for further details
- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual 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**

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.

Where we offer online services to pupils, such as classroom apps, and we need to rely on consent as a basis for processing, we request parental consent where the pupil is in the Primary School or under 13 in the Senior School (except for online counselling and preventive services).

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

7.2 Limitation, minimisation and accuracy

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so 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 if necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a 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 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

We are required, by law, to share certain information with specified external bodies as necessary, such as the local authorities, the Department for Education and the Independent Schools' Inspectorate.

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

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or by email to the Bursar. They should include:

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

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

9.2 Children and subject access requests

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

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carersof pupils in our Primary 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.

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 in our Senior School will 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- 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 e.g. if the request falls across a significant holiday and access to all information is not immediately possible.

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

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.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, 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)

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

10. Parental requests to see the educational record

All annual educational reports are sent directly and electronically to those with parental responsibility for the child to enable easy access and storage by the parent. A parent can request that such information be sent out again should it be necessary. Such a request should be sent in to the Head. As an independent school, our entrance examination and testing data remains confidential to the school and is not available to parents.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

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

12. Photographs and videos

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

We will obtain consent from parents/carers for photographs and video footage of their child to be used for communication, marketing and promotional materials. We will clearly explain how photographs and/or video footage will be used to the parent/carer. This consent is valid for the period of time the child attends the school and for up to three years afterwards.

Uses may include:

- On school collateral such as the school prospectus, e-newsletters and updates, hard copy newsletters or in other printed publications that we produce, on digital and wall displays etc.
- Outside of school by external agencies such as news media outlets, advertising campaigns and relevant organisations such as the GSA and IAPS
- Online on our school website and social media feeds

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or footage from our systems and not distribute it further. An up-to-date record of children for whom there is no consent in place to use photos or videos is maintained and shared with staff as required.

We may use group or class photographs or footage with very general labels e.g. 'U3 Rounders Team'. For news items about specific pupils, a photograph may be accompanied by the pupil's name. Images used on Social Media would not normally be accompanied by the pupil's full name without express permission.

See our Safeguarding Policy or request our Camera and Photography Policy for more information on our use of photographs and videos.

14. Data protection by design and default

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

- Ensuring the Head, the Bursar and the Governors have the necessary resources to fulfil their duties and maintain their expert knowledge about data protection
- 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
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- 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 Bursar 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, 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:

- Where paper-based personal information needs to be taken off site, e.g. data contained in markbooks, staff must ensure they keep it securely and return it to school as soon as possible
- The use of portable electronic devices by staff, such as laptops and hard drives to store/transport data, is not advised. Encrypted USB sticks are provided for staff/Governors, on request, and must be used for the purposes of transporting any necessary data safely but this is rarely necessary and staff/Governors will be advised of other safe options first.

- Staff should access such data as required from home via our online Home Access Plus system, which requires a secure password. Staff using a portable device of any description to access data or emails must ensure that the information they view cannot be accessed by any other person. Personal devices should be password protected.
- Staff, pupils or governors who need to store personal information on their personal devices, for a specific short-term purpose e.g. to work on a document, are expected to follow the same security procedures as for school-owned equipment (see our Online Safety Policy/ Staff ICT and Social Media Policy).
- Once a data document is no longer being worked on, it should be uploaded directly to the school system and not be stored on personal devices.
- 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 public access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- 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.

17. Personal data breaches

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

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

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

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

18. Training

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

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

19. Monitoring arrangements

The Bursar is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated as necessary, if any changes are made to the Data Protection Act 2018 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 board.

20. Links with other policies

This Data Protection Policy should be considered alongside the following school policies:

- Privacy Notice
- Online Safety Policy
- Safeguarding Policy

Other policies which exist to support this policy and are available on request from school include:

- Camera and Photography Policy GDPR and Exams – Policy
- Computing Rules and Online agreement - Primary
- Computing Rules and Online Agreement – Seniors
- Staff ICT and Social Media Policy
- Data Retention Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO. The Bursar will always liaise with the Head about any potential breach, unless the breach involves the Head. The Head will take the lead in the event of the Bursar being involved in a breach.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Bursar
- The Bursar will investigate the report, and determine whether a breach has occurred. To decide, the Bursar 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 Bursar/Head will alert the Chair of Governors to any data breach
- The Bursar/Head 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 Bursar/Head will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The Bursar/Head 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 Bursar/Head will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the Bursar/Head (whichever is the lead on the case) must notify the ICO.
- The Bursar/Head 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 securely in a designated Data Breach folder.
- Where the ICO must be notified, the Bursar/Head will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the Bursar/Head 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 either the Bursar or the Head, whichever is the lead contact for the case
    - 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 Bursar/Head 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 Bursar/Head expects to have further information. The Bursar/Head will submit the remaining information as soon as possible
- The Bursar/Head 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 Bursar/Head will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of either the Bursar or the Head, whichever is the lead contact for the case
    - 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 Bursar/Head 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 Bursar/Head 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 securely in a designated Data Breach folder.
- The Bursar, Head and Chair of Governors 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

In addition to reporting the breach to the ISO, we will take appropriate actions 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.

Possible actions could include:

- Recalling emails with sensitive data in them, either as individuals or with support from the Senior Network Manager
- Contacting anyone who has received sensitive data in error, with a request to delete it immediately and not share, publish, save or replicate the information in any way
- Requesting written confirmation that sensitive data, received in error, has been deleted
- Conducting an internet search to confirm that the information has not been shared and following up with the publisher of any material which still needs to be removed
- Reviewing staff training procedures and providing additional training as required