The Henrietta Barnett School

Data Protection Policy

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, 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:

- 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 UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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 our funding agreement and articles of association.

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.

TERM	DEFINITION
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 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 and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered with the ICO as 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 (DPO)

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

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

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

Our DPO is Joanna Avey, School Business Manager and is contactable via office@hbschool.org.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
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - 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 UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 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 i.e. 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 1 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

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- 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 or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

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.

Staff 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.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- 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 that 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.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Please see our separate privacy notices for information about which suppliers or contractors we regularly share personal data with.

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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Specific details of the information requested e.g. a child's personnel file, school medical records

If staff receive a subject access request in any form they must immediately forward it to the DPO.

9.2 Children and subject access requests

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

Children 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils 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 1 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. For example, pupils can pay for school dinners in cash at each transaction if they wish.

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.

For further detail about our biometric data, please see Appendix 2.

11. CCTV

We use CCTV in a small number of locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

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 Richard Cain, Site Manager.

12. Photographs and videos

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

- **educational use:** photography and videos taken for a variety of uses, such as school displays, assessment and workbooks. The principles of GDPR apply.
- **official school use:** photographs and videos which are used for the school's administrative, functional educational and pastoral purposes including archives. These images are likely to be stored electronically alongside other personal data. The principles of GDPR apply.
- **media use:** photography and videos which are intended for a wide audience (for example, photographs taken for School literature, marketing promotion and school's social media platforms). The principles of GDPR apply.

When photographs are taken for these reasons, we will explain to the pupil at the time what the purpose and use is.

We will obtain written consent from parents/carers for photographs and videos to be taken within school of pupils for these uses. Additionally, as children aged 12 and above are generally regarded to be mature enough to understand their rights, written consent will also be sought from students in Year 8 and above. When a student turns 18, their written consent, or withdrawal of it, will be the determining factor. If a child should not wish to be in a photograph, even where parental consent has been given, then this will be respected.

All parents/guardians will be asked to complete a consent declaration upon their child joining the School. This will determine whether or not their child is allowed to participate in photographs and videos for educational, administrative and media purposes. The consent form is valid for the period of time that the child attends the School, unless the pupil's circumstances change in any way or consent is withdrawn. All parents/guardians and students are entitled to withdraw or change their consent at any time but must do so in writing. To do this, they can email office@hbschool.org.uk, marking their email for the attention of the School Information and Data Manager. If there is a disagreement over consent, or if a parent does not respond to a consent request, it will be treated as though consent has not been given, and photos and videos will not be taken or published of the pupil in question. When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified unless explicit consent has been sought.

For any Local After Children (LAC) or adopted pupils, the Designated Safeguarding Lead (DSL) will liaise with the pupil's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of a LAC or adopted pupil would risk their security in any way. Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the DSL believe that taking photos or videos of such pupils would put their security at further risk, then the pupils will not be included.

Consent status will be stored and amended on the secure SIMS system, and the school's Data and Information Manager will produce regular reports for staff to consult in the shared drive, additionally updating the reports when advised of a change in consent. All staff planning to take or use photographs for the purposes outline above should consult the report of withheld consent.

If the School decides to use a professional photographer / design agency / videographer for official school photographs, videos and events, the member of staff responsible for booking the photographer will:

- Provide a clear brief for the photographer / design agency / videographer about what is considered appropriate in terms of content and behaviour
- Issue the photographer / design agency / videographer with identification which must be worn at all times
- Publicise at the time of the session that a photographer / design agency / videographer is working
- Not allow unsupervised access to pupils or one-to-one photography sessions
- Communicate to the photographer / design agency / videographer that the material may only be used for the School's own purposes and that permission has not been given for the photographs and/or videos to be used for any other purposes
- Ensure that the photographer / design agency / videographer will comply with GDPR requirements

See Appendix 3 for staff guidelines on how to approach photography and videoing of pupils.

Where an external company or provider requests to take and/or record photography or videos of students for their company's uses, they will be expected to abide by this policy and the lead member of school staff will seek consent from both parents and students on that occasion.

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. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The Henrietta Barnett School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Henrietta Barnett School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

15. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing 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 may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any

transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. Data security and storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept in locked areas when not in use, either at school or if being used offsite.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access, including when on the school site or when off it e.g. trip information.
- Passwords that are at least 12 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.
- 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 (see our IT Acceptable Use Agreement). 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)

17. 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.

18. 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 after becoming aware of it. Such breaches in a school context may include, but are not limited to:

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

19. 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.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices
- IT Acceptable Use Agreement
- Child Protection & Safeguarding Policies
- Remote Education Statement
- Staff Code of Conduct

Review & Update:
This Policy will be reviewed annually.
It was last reviewed in May 2025.

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by emailing them.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school network.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. 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 DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored on the school network
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will meet termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of data breaches if they were to occur, focusing especially on an example of sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the school's network manager or external IT manager to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it is appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the DSL and discuss whether the school should inform any, or all, of its safeguarding partners.

Appendix 2: School Use of Biometric Data

Introduction

In 2017, the School started using a biometric cashless system (from Biostore) for paying for purchases in the canteen. This policy is to confirm our approach to use of biometric data.

The School complies with the General Data Protection Regulations (GDPR) and with the guidance given by the relevant government guidance (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf) and by the Information Commissioner's Office regarding the use of biometric data.

Fingerprint images are not stored by the system (instead, a set of coordinates is translated into a string of letters/numbers and encrypted). The encryption method used by the system is a high level, industry standard method. The data held could not be used to recreate a fingerprint image, nor could it be used in a forensic investigation.

The School offers an opportunity to opt out for those students who, upon consideration, feel that they would rather not have their biometric data recorded.

Cashless System

A cashless system allows parents to top up their child's account before entering the canteen, which allows for quicker serving times. The system recognises each individual student, holds individual cash balances, records cash spent and cash received, on what food, on any specific date and time of day.

How are students recognised by the system?

Each student has their fingerprint registered which is then translated to an Alpha Numeric number. The image is then discarded. When used, this will then enter them into the system program and identify them by a number.

How is this then used to obtain a school meal?

The Student places their finger on a scanner at the point of sale; a display will show the server the student's name, class and current cash balance held within the system. The selected food items will be entered into the system from an itemised keyboard while the amount spent and the new cash balance will show on the display.

How is money entered into the system?

Online Payments are made by parents (and staff) via the School's ParentMail system. The parent / guardian logs on using a secure user-name & password to 'top-up' their child's account online (or each child's account, where families have more than one child at the school). Parents can elect to automatically top up when a child's account drops below a certain level.

How does a student check what is their current balance?

A Remote Display at the point of sale will show the new cash balance when the food service is finished.

Is there a daily spend limit?

The system has a daily spend limit (currently £10) so parents know that the whole balance cannot be spent all in one day.

What if the student does not hold a sufficient cash balance one day to pay for a school dinner?

As before, no student is refused a school dinner because they have not brought their dinner money to school with them. Where a student does not have sufficient balance to pay for the meal they will be sent to the school office where a parent will be contacted. The system refreshes every 5 minutes therefore once the parent has topped up the student will then be able to go back to the canteen to buy lunch.

What about students entitled to a 'free school meal'?

The system works exactly the same for all students whether they pay or have a free school meal. All students have their own account to use in exactly the same way. The amount allocated for the free school meal will be entered into the system by the software daily. The system will then allow on a daily basis the required cash amount for each individual student to be allotted to their current cash balance. However, any under spend or missed lunch will be identified by the system and will not be added to the next day's balance. The student /parent can also add extra cash on to their balance in the system if they want to do so, by using ParentMail to enable a greater daily spend on the school dinner than allocated by their free meal allowance.

Data Handling

Certain data will be held on the system to enable accurate operation. This will include the student's name, class, account balance and meal entitlement. This data will be handled under the GDPR guidelines and only used by parties directly involved with the implementation of the system, and for that purpose. If you have any concerns please contact the School Business Manager.

Benefits of the Biometric Cashless System

* Convenient way of paying for school meals. No more looking for change every morning.
* Discourages the misuse of school dinner money through spending in shops outside of the school grounds.
* Alleviates many of the associated problems with the use of cash in schools. i.e. loss, theft, etc.
* Healthy eating is encouraged.
* Queuing times are reduced through increased speed of service.
* Automatic free meal allocation with the student remaining anonymous.
* Detailed reports to analyse all aspects of the use of the system.
* Having control of student accounts by students using the Fastrak System teaches important life skills.
* A more efficient delivery of service helps the caterer to provide wholesome, healthy and enjoyable school meals at a low cost.

Appendix 3: General Principles and Procedures for Photography and Video of Students in School

- Photographs and videos will be carefully planned before any activity.
- The list of all pupils of whom photos and videos must not be taken will be checked by the member of staff responsible for the activity in advance.
- Only pupils for whom consent has been given will be able to participate in the photography or video.
- Only School equipment will be used to take photographs and videos of pupils.
- When organising photography and videos of pupils, staff members involved will consider the following:
  • Can classroom or group shots be used rather than shots of individual pupils?
  • Are pupils suitably dressed to be photographed and videoed?
  • Do pupils selected for the photos and/or video reflect the diversity of the school?
  • Are the photos and/or videos totally necessary or could alternative methods be used for the same purpose? For example, could an article be illustrated by the work of the pupils rather than the pupils themselves?
- Only photos and videos of pupils in suitable dress will be taken/used.
- Children in swimming costumes are not to be photographed unless they are in the swimming pool.
- Where pupils are in PE kit, the focus should be on the activity and close up shots should be avoided.
- Photography and videos will only be taken in adequately supervised areas.
- Members of staff should not take one-to-one photos/videos of pupils unless in a public area.
- Photos and videos that may cause distress, upset and embarrassment will not be used.
- Photos and videos will be stored centrally and securely by the school at the earliest possible opportunity and then removed from the device used promptly.
- Staff will not use any personal devices to take photographs or videos of pupils.
- Photographs and videos taken by staff members may be used for educational purposes only where the appropriate consent is in place.
- Photographs and videos held on the school's storage drives are accessible to only members of staff for whom it is deemed access is a necessary part of their role.
- The school will not take or use photos or videos of any pupil that is subject to a court order.