The Free School Norwich

Data Protection Policy

Contents

1. Aims

2. Legislation and guidance

3. Definitions

4. The data controller

5. Accountability

6. Roles and responsibilities

7. Data protection principles

8. Collecting personal data

9. Sharing personal data

10. Subject access requests and other rights of individuals

11. Parental requests to see the educational record

12. Biometric recognition systems

13. CCTV

14. Photographs and videos

15. Artificial intelligence (AI)

16. Data protection by design and default

17. Data security and storage of records

18. Disposal of records

19. Personal data breaches

20. Training

21. Monitoring arrangements

22. Links with other policies

Appendix 1: Personal data breach procedure

Appendix 2: Data retention schedule

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, Trustees, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

term	definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation

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, Trustees, visitors and others, and therefore is a data controller.

The school is registered with the ICO, as legally required.

5. Accountability

The school will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR and DPA, and will provide comprehensive, clear and transparent privacy policies. The school will also provide evidence that it is complying with UK GDPR and DPA.

Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.

Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The school will also document other aspects of compliance with the UK GDPR and DPA where this is deemed appropriate in certain circumstances by the DPO, including the following:

- Information required for privacy notices, e.g. the lawful basis for the processing
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessment (DPIA) reports
- Records of personal data breaches

The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Minimising the processing of personal data.
- Pseudonymising personal data as soon as possible.
- Ensuring transparency in respect of the functions and processing of personal data.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

DPIAs will be used to identify and reduce data protection risks, where appropriate.

6. 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 Trust Board

The Trust 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.

Where requested the DPO will provide an annual report of their activities directly to the Trust 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 The School DPO Service and is contactable via office@schoolDPOservice.com

5.3 Principal

The Principal 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

7. 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.

8. 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 data retention schedule in Appendix 2.

9. 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 children or 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.

International transfers of personal data are not routine within the school environment; however, where personal data is transferred outside the UK as a result of third-party or cloud-based systems, such transfers shall take place only where legally permitted. Any international data transfer shall be supported by appropriate safeguards and fully documented to demonstrate compliance with UK GDPR requirements.

10. 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
- Details of the information requested

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 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 carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil’s ability to understand their rights will always be judged on a case-by-case basis.

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.

9.5 Data Subject Access Rights and Regulatory Consequences

The Trust recognises its statutory obligation to comply fully with data subject rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This includes, but is not limited to, the right of individuals to request access to their personal data through a Subject Access Request (SAR).

All Subject Access Requests will be identified promptly, handled lawfully, and responded to within the statutory timescales set out in legislation. Requests will be escalated without delay to the Data Protection Officer where they are complex, involve exemptions, relate to safeguarding or special category data, or where there is uncertainty regarding the Trust's legal obligations.

Failure to comply with data subject access rights may result in individuals raising complaints with the Information Commissioner's Office (ICO). Regulatory action by the ICO may include enquiries or investigations, formal reprimands, enforcement notices requiring changes to policies, procedures or practices, and, in more serious or persistent cases, the imposition of financial penalties.

All staff have a responsibility to take data subject rights seriously, to recognise requests that may constitute a Subject Access Request regardless of format, and to escalate such requests promptly in line with this policy.

Timely escalation to the Data Protection Officer is essential to ensure the Trust meets its legal obligations and demonstrates accountability under UK data protection law.

11. Parental requests to see the educational record

As a free school, there is no automatic parental right of access to the educational record.

12. Biometric recognition systems

The Free School Norwich does not use any biometric recognition systems at this time.

13. CCTV

We use CCTV in various 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.

14. Photographs and videos

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

Parents provide consent on the initial registration form. These registration forms are scanned into our MIS Arbor and linked to the child record. Where consent is required for external publication of images eg. social media, business promotional material etc. parents are contacted directly on each occasion and this consent is recorded as a note on the child record within Arbor. Where consent is not given or withdrawn, a record is made on child's record within Arbor.

Where parental consent has been provided, the School reserves the right to use photographs and video images of pupils for legitimate school purposes, including display on the School website, within school publications, and in photographs displayed around the School premises. Unless consent is withdrawn, this may include the continued use of images of pupils after they have left the school, where such use remains consistent with the purposes for which consent was originally given. Parents and carers retain the right to withdraw consent at any time including after the child has left the school. Requests to withdraw consent must be made in writing and should, where possible, specify the location or context in which the image is used to enable the School to take timely and appropriate action.

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 have agreed to this.

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.

15. Artificial intelligence (AI)

The school recognises that artificial intelligence tools, including generative AI and other automated tools, may support teaching, learning and efficiency. However, their use can also create risks to personal data, safeguarding, confidentiality, accuracy and fairness.

The school may use AI tools where these have been reviewed and approved by the school. Approval will take into account, where relevant:

- the purpose of the tool and whether its use is necessary and proportionate
- whether the tool processes personal data, special category data or criminal offence data
- whether there is an appropriate lawful basis for any processing
- whether personal data entered into the tool is used to train the provider's model or shared with third parties
- the age restrictions, safeguarding implications and suitability of the tool for pupils
- the technical and organisational security measures in place
- whether a data protection impact assessment is required
- whether privacy notices or other transparency information need to be updated
- whether staff and pupils require training or additional guidance on safe use

Staff, governors, pupils and any other users must not enter personal data, special category data, safeguarding information, confidential school information or other sensitive information into any AI tool unless the tool has been approved for that purpose and the school is satisfied that appropriate safeguards are in place.

Where personal data is used in connection with an approved AI tool, the school will ensure that such use complies with UK data protection law, including the data protection principles, and that individuals are informed as required through the school's privacy information.

The use of AI outputs must be subject to appropriate human review. AI tools must not be relied upon as the sole basis for significant decisions about pupils, parents, carers, staff or governors unless the school has ensured that such processing is lawful and that appropriate safeguards are in place.

Any member of staff wishing to introduce or trial a new AI tool, or to use an approved AI tool in a new way involving personal data, must seek approval from the headteacher and/or data protection officer before use.

Any suspected personal data breach involving an AI tool must be reported immediately in accordance with this policy and the school's personal data breach procedure.

16. 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

17. 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:

- 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, photocopiers/printers or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff are required to take extra precautions.
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.

- Staff, pupils or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety Policy and ICT Acceptable Use 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 (see section 9)

18. 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.

19. 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

20. Training

All staff and Trustees 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.

21. Monitoring arrangements

The DPO is responsible for notifying the school of any substantive changes required to the policy.

This policy will be reviewed and approved every two years when substantive changes are made and approved by the full Trust Board.

22. Links with other policies

This data protection policy is linked to our:

- Privacy notices
- E-Safety Policy
- ICT Acceptable Use Policy
- Safeguarding Policy

Approval level: Trust Board

Approved date: May 2026

Policy Review Date: May 2028

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, Trustee or data processor must immediately notify the data protection officer (DPO) by phone or email.

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 Trustees 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 School Business Manager.

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 remotely and secured by the DPO.

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)

The DPO and Principal 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 set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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)

- 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 IT support provider 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's 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 endeavor 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 designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with Trustees
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix 2: Data retention schedule

Management Data				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Board of Trustees – general correspondence	Close at end of current school year	Current year + 3 years		Destroy
FGB Meetings Minutes (master)	Close at end of current school year	10 years from the date of the meeting		Destroy
Senior Management Team-Meeting Minutes	Close at end of current school year	Date of meeting + 5 years		Destroy
Staff Meeting Minutes	Close at end of current school year	Normal Review		Determination on Review
School Development Plan	Retain whilst valid – close when superseded	Life of the plan + 3 years		Destroy
Curriculum Policies	Retain whilst valid – close when superseded	Until superseded		Keep 1 copy of previous policies and destroy all others
Policy Statements (Data Protection, Internet, Health & Safety, Child Protection, Equality etc.)	Retain whilst valid – close when superseded	Review regularly & retain latest version Older versions: date of expiry + 1 year		Destroy
PTA – minutes and general correspondence	Close at end of current school year	Normal Review		Determine on Review
Visitors Book	Close at end of current school year	End of current year + 1 years		Destroy
Circulars to Staff, Parents and Pupils	Close at end of current school year	End of current year + 2 years		Destroy

Comments/Complaints	Close at end of current school year	Date of resolution of complaint + 6 years		Archive
Annual Report	Issued every academic year	Date of Report + 10 years		Permanent Preservation
School Fund	Close at end of current financial year	Current financial year + 6 years		Destroy
Emergency Planning/Business Continuity Plan	Retain whilst valid – close when superseded	Until superseded		Destroy
CCTV	Overwritten automatically	30 days	Surveillance Camera Code of Practice 2021	Delete
Pupil				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Pupil file and records that contribute to the pupil record	Close when child leaves setting and either archived or sent to child's onwards destination	Primary - Retain whilst the child remains at the primary school Secondary - Date of birth of the pupil + 25 years	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437 As amended by SI 2018 No 688 Limitation Act 1980 (Section 2)	
Pupil Admission Data	Close when register ceases to be used	Date of admission + 1 year	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools' adjudicators and admission appeals panels December 2014	Destroy
Proofs of address supplied by parents as part of the admissions process	Added to pupil file	Current year + 1 year		
Applications for enrolment	Close at end of school year in which application received	1 year from date of application		Destroy

Pupil Attendance Registers electronic	Close when register ceases to be used	3 years after the date on which the entry was made.	School attendance: Departmental advice for maintained schools, Academies, independent schools and local authorities 2014	Destroy
Pupil Education Records - School/Progress Reports etc.	Close when pupil leaves school	Lifetime of pupil file		Destroy
Special Education Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Close when pupil leaves school	Date of birth of the pupil + 31 years [Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan in line with the Limitation Act]	Children and Family's Act 2014; Special Educational Needs and Disability Act 2001 Section 14	Destroy
Child Protection	Retain in secure, confidential storage	Until Pupil is 25 years old	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	Destroy
Disciplinary Action (Suspension/Expulsion)/Offences – bullying	Close when pupil leaves school	Lifetime of pupil file		Destroy
Timetables + Class Groupings	Close at end of current academic year	Current School year + 1 Year		Destroy
Examination Results	Close at end of current academic year	Current School Year + 6 years		Destroy

Careers Advice	Added to pupil file	Life of pupil file		Destroy
School Meals returns	Close at end of current financial year	Current financial year + 6 years		Destroy
Free School Meal registers	Close at end of current financial year	Current financial year + 6 years		Destroy
School Trips – Financial & Administration details	Close at end of current financial year	Current financial year + 6 years		Destroy
School Trips-Attendance/Staff Supervision etc	Close on completion of trip	School may wish to complete a risk assessment to assess whether the forms are likely to be required and could decide to dispose of the consent forms at the end of the trip (or at the end of the academic year).		Destroy
Reports of Stolen/Damaged Items	Close at end of current academic year	7 years		Destroy
Medical Records – records of pupils with medical conditions and details for the administration of drugs when necessary.	Close when pupil leaves school	Until pupil is 22 years old or in the case of a Special Needs pupil, until 25 years old		Destroy
Personnel				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Staff Personnel Records (including recruitment, interview notes, appointment details, training, staff development etc.)	Close when member of staff leaves school	During validity + 6 years after leaving employment	Limitation Act 1980 (Section 2)	Destroy

Staff Salary Records	Close at end of current financial year	Last Day of Employment + 85 Years		Archive for Pension purposes
Staff Sickness Records (copies of Medical Certs)	Close at end of current academic year	Current academic year + 6 years		Destroy
Substitute Teacher Records	Close at end of current academic year	Current academic year + 6 years		Destroy
Substitute Staff Records-non teaching (cover for nursery assistants)	Close at end of current academic year	Current academic year + 6 years		Destroy
Student Records-non teaching (e.g. nursery assistant students & pupils from schools on work experience)	Close at end of current academic year	Current academic year + 6 years		Destroy
Student Teachers on Teaching Practice – student teacher progress	Close at end of current academic year	Current academic year + 6 years		Destroy
Procedures for Induction of Staff		Until superseded		Destroy
Staff/Teacher's Attendance Records	Close after leaving employment	7 years after leaving		Destroy
Staff Performance Review	Close at end of review period covered	During validity		Destroy
Records relating to any allegation of a child protection nature against a member of staff		Until the person's normal retirement age or 10 years from the date of the allegation (whichever is the longer) then REVIEW.	"Keeping children safe in education Statutory guidance for schools and colleges September 2018"; "Working together to safeguard children. A guide to inter-agency working to safe-guard and promote the welfare of children 2018"	

Finance				
Record	**File Action**	**Minimum Retention Period**	**Statutory Provision**	**Action After Retention**
Annual Budget	Close at end of current financial year	Current financial year + 6 years		Destroy
Budget Monitoring	Close at end of current financial year	Current financial year + 3 years		Destroy
Annual Statement of Accounts (Outturn Statement)	Close at end of current financial year	Current financial year + 6 years		Archive
Order Books, Invoices, Bank Records, Cash Books, Till Rolls, Lodgment books etc.	Close at end of current financial year	Current financial year + 6 years		Destroy
Postage Book	Close at end of current financial year	Current financial year + 6 years		Destroy
Purchasing – Tender Information & Prices		Until superseded		Destroy contract schedules when they expire.
Audit Reports	Close at end of current financial year	Current financial year + 6 years		Destroy
All records relating to the management of contracts under signature		Last payment on the contract + 6 years	Limitation Act 1980	Destroy contract when they expire.
Health and Safety				
Record	**File Action**	**Minimum Retention Period**		**Action After Retention**
Accident / Incident Book	Close after last entry in book	Date of closure + 12 years	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992	Destroy
Legal /Accident/Incident Forms		Until pupil is at least 22 years old or in the case		Destroy

		of an adult 4 years from the date of the accident	Section 8. Limitation Act 1980 Social Security (Claims and Payments) Regulations 1979. SI 1979 No 628 Social Security (Claims and Payments) Regulations SI 1987 No 1968 Revokes all but Part 1 of SI 1979 No 628 Social Security Administration Act 1992 Section 8. Social Security (Claims and Payments) Amendment (No 30 Regulations 1993 SI 1993 No 2113 Allows the information to be kept electronically	
Risk Assessments – work experience locations/pupils		Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred		Destroy
H & S Reports		Current Year + 20 years		Destroy
Fire Procedure		Until superseded		Retain copies of earlier versions
Security System File		For the life of the system		Destroy
HS Policy Statement		Date of expiry + 1 Year		Destroy