WADE DEACON TRUST

A COMMITMENT TO EXCELLENCE

# DATA PROTECTION POLICY

**Policy Number:** 73
**Version Number:** 06
**Ratified by Trustees:** 22rd April 2026
**Next Review Date:** 22rd April 2027
**Link:** Mr J Lowe

A GREAT PLACE **TO BE A PART OF**

## STATEMENT OF INTENT - DATA PROTECTION POLICY

This policy should be implemented within the context of the vision, aims and values of each of our academies.

Each academy within the Wade Deacon Multi Academy Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK version of the GDPR (UK-GDPR), which came in to force on 1st January 2021, the Data Protection Act 2018 (DPA 2018) and the Data (Use and Access) Act 2025 (DUA) which received Royal Assent on 19 June 2025.

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

This policy will be reviewed as it is deemed appropriate, but no less frequently than every year by the Trustees'. The policy will be promoted and implemented within each academy.

## 1. LEGISLATION AND GUIDANCE

1.1. This policy meets the requirements of the UK-GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK-GDPR.

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

1.3. 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.

## 2. DEFINITIONS

| Term | Definition |
|---|---|
| Personal data | Any information relating to an identified, or identifiable, individual.<br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br>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:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• 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.<br>Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | A person or organisation that determines the purposes and the means of processing of personal data. |
| Data processor | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

## 3. THE DATA CONTROLLER

3.1. The Trust and its academies process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

3.2. The Trust is registered with the ICO and will renew this registration annually or as otherwise legally required.

## 4. ROLES AND RESPONSIBILITIES

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

### 4.2. Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

### 4.3. Local Governing Committees

Local Governing Committees have responsibility for ensuring that each Academy complies with all relevant data protection obligations.

### 4.4. Data Protection Officer

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

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, 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 Mr Nick Holden, (NexusProtect) and is contactable on 07469 193981 or governance@nexus-global.co.uk

### 4.5. Principal

The Principal of each Academy acts as the representative of the data controller on a day-to-day basis.

### 4.6. All Staff

Staff are responsible for:

4.6.1. Collecting, storing and processing any personal data in accordance with this policy

4.6.2. Informing their school of any changes to their personal data, such as a change of address

4.6.3. Contacting the DPO in the following circumstances:

4.6.3.1. With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure

4.6.3.2. If they have any concerns that this policy is not being followed

4.6.3.3. If they are unsure whether or not they have a lawful basis to use personal data in a particular way

4.6.3.4. 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

4.6.3.5. If there has been a data breach

4.6.3.6. Whenever they are engaging in a new activity that may affect the privacy rights of individuals

4.6.3.7. If they need help with any contracts or sharing personal data with third parties

## 5. DATA PROTECTION PRINCIPLES

The UK-GDPR is based on data protection principles that our Trust must comply with. The principles say that personal data must be:

5.1. Processed lawfully, fairly and in a transparent manner

5.2. Collected for specified, explicit and legitimate purposes

5.3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

5.4. Accurate and, where necessary, kept up to date

5.5. Kept for no longer than is necessary for the purposes for which it is processed

5.6. Processed in a way that ensures it is appropriately secure

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

## 6. COLLECTING PERSONAL DATA

### 6.1. Lawfulness, fairness and transparency

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

6.1.1.1. The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract

6.1.1.2. The data needs to be processed so that the Trust can **comply with a legal obligation**

6.1.1.3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

6.1.1.4. The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest or exercise its official authority

6.1.1.5. The data needs to be processed for the **legitimate interests** of the Trust (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

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

6.1.2. For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

6.1.2.1. The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

6.1.2.2. The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

6.1.2.3. 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

6.1.2.4. The data has already been made **manifestly public** by the individual

6.1.2.5. The data needs to be processed for the establishment, exercise or defence of **legal claims**

6.1.2.6. The data needs to be processed for reasons of **substantial public interest** as defined in legislation

6.1.2.7. 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

6.1.2.8. 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

6.1.2.9. 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

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

6.1.3.1. The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**

6.1.3.2. 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

6.1.3.3. The data has already been made **manifestly public** by the individual

6.1.3.4. 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**

6.1.3.5. The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

6.1.5. 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.

6.2. Limitation, minimisation and accuracy

6.2.1. 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.

6.2.2. 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.

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

6.2.4. We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

6.2.5. 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 Trust's record retention policy.

## 7. SHARING PERSONAL DATA

7.1. We routinely share personal data with our suppliers and other 3rd parties according to the lawful bases set out above. These circumstances include, but are not limited to, situations where:

7.1.1. There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

7.1.2. We need to liaise with other agencies – we will seek consent as necessary before doing this

7.1.3. 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:

7.1.4. Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

7.1.5. Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share

7.1.6. Only share data that the supplier or contractor needs to carry out their service

7.2. We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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

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

## 8. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

### 8.1. 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:

8.1.1. Confirmation that their personal data is being processed

8.1.2. Access to a copy of the data

8.1.3. The purposes of the data processing

8.1.4. The categories of personal data concerned

8.1.5. Who the data has been, or will be, shared with

8.1.6. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

8.1.7. The right to lodge a complaint with the ICO or another supervisory authority

8.1.8. The source of the data, if not the individual

8.1.9. Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

8.1.10. The safeguards provided if the data is being transferred internationally

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

8.1.11.1. Name of individual

8.1.11.2. Correspondence address

8.1.11.3. Contact number and email address

8.1.11.4. Details of the information requested

8.1.12. If staff receive a subject access request in any form they must immediately forward it to the school's Data Lead.

### 8.2. Children and subject access requests

8.2.1. 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.

8.2.2. 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.

8.2.3. 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.

## 8.3. Responding to subject access requests

8.3.1. When responding to requests, we:

8.3.1.1. May ask the individual to provide 2 forms of identification

8.3.1.2. May contact the individual via phone or email to confirm the request was made by them

8.3.1.3. May 'stop the clock' while seeking clarification from the requester, especially where the request is unclear. The time limit for responding will be paused until such clarification is received.

8.3.1.4. Will only conduct 'reasonable and proportionate' searches and may choose not to supply information which the requester already holds or has access to.

8.3.1.5. 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)

8.3.1.6. Will provide the information free of charge

8.3.1.7. May tell the requester we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the requester of this within 1 month, and explain why the extension is necessary

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

8.3.2.1. Might cause serious harm to the physical or mental health of the pupil or another individual

8.3.2.2. 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

8.3.2.3. 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

8.3.2.4. 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

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

8.3.4. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

8.3.5. 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.

### 8.4. Other data protection rights of the individual

8.4.1. 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:

8.4.1.1. Withdraw their consent to processing at any time

8.4.1.2. Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

8.4.1.3. Prevent use of their personal data for direct marketing

8.4.1.4. Object to processing which has been justified on the basis of public interest, official authority or legitimate interests

8.4.1.5. Challenge decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

8.4.1.6. Be notified of a data breach in certain circumstances

8.4.1.7. Make a complaint to the ICO

8.4.1.8. Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

8.4.2. 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 school's Data Lead.

## 9. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

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

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

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

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

## 10. CCTV

10.1. We use CCTV in various locations around some school sites to ensure they remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

10.3. Individuals have the right to request details of the images of them being held

10.4. Any enquiries about the CCTV system should be directed to the School Business Manager at the school site.

## 11. DATA PROTECTION AND ARTIFICIAL INTELLIGENCE (AI)

11.1. The use of Artificial Intelligence (AI) and Machine Learning (ML) tools, including Generative AI, introduces specific data protection risks. The Trust is committed to using AI responsibly, ethically, and in a way that safeguards personal data.

11.2. Principles for AI Use

11.2.1. Approval and Due Diligence: Only Trust-approved AI tools may be used for processing school-related personal data. Before procuring or implementing a new AI system, a thorough Data Protection Impact Assessment (DPIA) must be completed and approved by the DPO and Senior Leadership, especially if the tool involves high-risk processing, special category data, or automated decision-making.

11.2.2. Lawful Basis: The Trust must identify and document a clear lawful basis under UK GDPR for any AI-related processing of personal data.

11.2.3. Data Minimisation: Where possible, AI tools should be used with anonymised or pseudonymised data. Staff and pupils must not input identifiable personal data (e.g., names, addresses, pupil work containing personal identifiers, sensitive information) into open/public Generative AI tools (like most free chatbots) as this data may be used by the provider to train their models.

11.2.4. Transparency and Fairness: Where AI is used to assist in decision-making that significantly affects an individual (e.g., a grading assessment or pastoral support recommendation), this use must be transparently communicated to the data subject. The school must monitor the AI system for potential bias or discriminatory outputs, particularly in relation to protected characteristics.

11.2.5. Human Oversight: AI systems must not be used to make fully automated decisions that produce legal or similarly significant effects on pupils or staff without significant and effective human review and intervention. Human judgement must remain the final authority, and individuals must have the right to request a human review of an AI-assisted decision.

11.3. Staff and Pupil Guidance on AI

11.3.1. Staff Use:

11.3.2. Staff must only use AI tools for work purposes that have been vetted and approved by the Trust.

11.3.3. Any content or data generated by AI must be fact-checked and reviewed for accuracy, bias, and appropriateness before use, particularly if it involves pupil assessments, external communications, or administrative tasks.

11.3.4. Pupil Use:

11.3.5. Pupil use of AI tools must comply with the school's Acceptable Use Policy and Online Safety Policy.

11.3.6. Pupils must be educated on the risks of entering personal information into public AI tools.

11.3.7. Guidelines on academic integrity and plagiarism related to AI-generated work will be clearly communicated.

## 12. PHOTOGRAPHS AND VIDEOS

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

12.2. We will obtain written consent from parents/carers, or pupils if aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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

12.3.1. Within school on notice boards and in school magazines, brochures, newsletters, etc.

12.3.2. Outside of school by external agencies such as the school photographer, newspapers, campaigns

12.3.3. Online on our Trust/school website or social media pages

12.4. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

## 13. 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

13.1. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

13.2. 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)

13.3. 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)

13.4. Integrating data protection into internal documents including this policy, any related policies and privacy notices

13.5. 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

13.6. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

13.7. Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply

13.8. Maintaining records of our processing activities, including:

13.8.1. For the benefit of data subjects, making available the name and contact details of our school Data Protection Lead and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)

13.8.2. 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure

## 14. 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:

14.1. 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

14.2. Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

14.3. Where personal information needs to be taken off site, staff must sign it in and out from the school office

14.4. Passwords that are at least 8 characters long containing letters, numbers and symbols are used to access Trust/school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

14.5. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

14.6. Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust/school-owned equipment (see our Information and Communication Systems Policy)

14.7. 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)

## 15. DISPOSAL OF RECORDS

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

15.2. 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.

## 16. PERSONAL DATA BREACHES

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

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

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

16.3.1. A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium

16.3.2. Safeguarding information being made available to an unauthorised person

16.3.3. The theft of a Trust/school laptop containing non-encrypted personal data about pupils

## 17. TRAINING

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

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

## 18. COMPLAINTS PROCESS

18.1. Should you wish to make a complaint regarding how your data is being handled, stored or processed or about anything else covered in this policy please contact the **Data Lead in school**, in the first instance.

18.2. Any complaint will be acknowledged within 30 days and will be responded to without undue delay.

## 19. MONITORING ARRANGEMENTS

19.1. This policy will be monitored and reviewed every two years, or in light of any changes to relevant legislation by the DPO.

19.2. The DPO will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.

19.3. The Principal will communicate changes to this policy to all members of staff.

## 20. LINKS WITH OTHER POLICIES

20.1. This data protection policy is linked to our:

20.1.1. Freedom of Information Policy & publication scheme

20.1.2. Information and Communication Systems Policy

20.1.3. Record Retention Policy

20.1.4. Protection of Biometrics Policy

20.1.5. Artificial Intelligence (AI) Policy

20.1.6. Academy CCTV Policy

20.1.7. Academy Child Protection Policy

## APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the School Data Protection Lead or DPO
- The School Data Protection Lead or DPO will investigate the report and determine whether a breach has occurred. To decide, the School Data Protection Lead or 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
- The School Data Protection Lead or DPO will alert the Principal and the Director of Operations
- The School Data Protection Lead or DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The School Data Protection Lead or DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out:
    - 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. 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
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- As above, any decision on whether to contact individuals will be documented by the DPO.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - 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 under a separate file held by the Headteacher or Data Lead.
- 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

Actions to minimise the impact of data breaches

We will take action to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Relevant Actions:

- Passwords are used to access computers.
- Passwords are not shared.
- If a computer is left unattended for any period then the operator will lock their screen.
- Information passed onto other schools will be done securely and receipts will be retained. Any safeguarding information will be sent in a separate envelope marked for the attention of the Headteacher or Designated Safeguarding Officer.
- School operate a tidy desk policy to ensure no sensitive data is left on view.

Special category data (sensitive information) being disclosed via email (including safeguarding records)

If special category data 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 ICT department to recall it

In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will ensure we receive 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

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 governors

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