

# **DATA PROTECTION POLICY**

**Dormers Wells Learning Trust**

<b>Ratified by Governors</b>	October 2025
<b>Review Date</b>	October 2026
<b>Staff Responsible</b>	Mr Y Parmar

## Contents

1. Aims.....	3
2. Legislation and guidance .....	3
4. The data controller .....	5
5. Roles and responsibilities .....	5
6. Data protection principles.....	6
7. Collecting personal data.....	6
8. Sharing personal data .....	8
9. Subject access requests and other rights of individuals .....	9
10. Parental requests to see the educational record .....	11
11. CCTV .....	11
12. Photographs and videos .....	12
13. Data protection by design and default .....	12
14. Data security and storage of records.....	12
15. Disposal of records .....	13
16. Personal data breaches .....	13
17. Training.....	13
18. Monitoring arrangements .....	13
19. Links with other policies .....	13

## 1. Aims

This policy applies to the schools within Dormers Wells Learning Trust, namely Dormers Wells Primary School and Dormers Wells High School.

The Trust and our schools aim to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018.

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

This policy does not form part of any individual's terms and conditions of employment with the Trust or individual schools and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves and comply with safe working practices commensurate with this policy via data protection training and information bulletins. Breach of the Data Protection Policy may be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

The Trust is registered with the Information Commissioner's Office (ICO) as required; registration number: ZA315865.

## 2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the provisions of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

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

In addition, this policy complies with our funding agreement and articles of association.

## 3. Definitions

<b>Personal data</b>	<p>Any information relating to an identified, or identifiable, individual. We may be able to identify the individual from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p>

	<ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>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. Processing also includes transmitting or transferring personal data to third parties.</p>
<b>Automated Processing</b>	<p>Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.</p> <p>An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.</p>
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

<b>Data Protection Impact Assessment (DPIA)</b>	DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.
---	---

#### 4. The data controller

The Trust and schools process personal data relating to parents, students, staff, governors, visitors and others, and therefore are data controllers.

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

#### 5. Roles and responsibilities

This policy applies to all staff employed by the Trust or schools, 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

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 Trust or individual school data protection issues.

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

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Judicium Education and are contactable via Judicium Consulting Ltd, 5th Floor, 98 Theobalds Road. Alternatively they can be contacted by telephone: 0345 548 7000 (option 1, then option 1 again).

The key persons for initially contacting with regards to data protection issues in each school in Dormers Wells Learning Trust before contacting the DPO are:

- Dormers Wells Primary School: Ellie Mosley on 020 8574 6999 or 020 8571 1230 or [dwijadmin@dwij.co.uk](mailto:dwijadmin@dwij.co.uk)
- Dormers Wells High School: Yatish Parmar on 020 8566 6446 or [info@dwhs.co.uk](mailto:info@dwhs.co.uk)

##### 5.3 Headteacher

The Executive 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 Trust or relevant 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 European Economic Area

- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

## **6. Data protection principles**

The UK GDPR is based on data protection principles that our Trust and schools 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 to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

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

## **7. Collecting personal data**

### **7.1 Lawfulness, fairness and transparency**

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

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carers when appropriate in the case of a student) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services). Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the Trust or school will normally seek another legal basis to process that data. However, if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

The Trust or school will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. The Trust or school will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data. Data Subjects have a responsibility to ensure data is accurate, up to date and relevant.

## **7.2 Limitation, minimisation and accuracy**

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

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's records management policy.

## **7.3 Security**

In order to assure the protection of all data being processed, the Trust and its schools will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption
- Pseudonymisation (this is where information that directly or indirectly identifies an individual is replaced with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure)
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it)
- Adhering to confidentiality principles and implementing processes that ensure the safe collection and destruction of data were required;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follows procedures and uses technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Further details on the Trust's security measures are set out in the eSafety, Cybersecurity and Information Security Policies.

## **7.4 Transparency and Privacy Notices**

The Trust and schools will provide detailed, specific information to data subjects. This information will be provided through the Trust's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices set out information for data subjects about how the Trust or schools use their data and the Trust's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the data protection officer, the Trust or school's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our staff privacy notice.

When personal data is collected indirectly (for example from a third party or publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. The Trust or school will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as “children” under the UK GDPR.

## **8. Sharing personal data**

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

- There is an issue with a student 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 if sharing is not compliant with the original privacy notice.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us
  - Consider whether sharing the personal data complies with the privacy notice that has been provided to the data subject

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for (but not limited to):

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We 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 students or staff.

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

### **8.1 Artificial Intelligence**

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, Copilot and Gemini. The Trust and its schools recognise 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 Trust or its schools will treat this as a data breach and will follow the personal data breach procedure outlined in section 16. Further information can be found in each school's AI policy.



## **9. Subject access requests and other rights of individuals**

### **9.1 Subject access requests**

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- Request a copy of an agreement under which personal data is transferred outside of the EEA
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

Subject access requests must be submitted in writing, either by letter, email or fax to the nominated contact at either the Trust, or the individual school as designated in section 5.2. They should include:

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

If staff receive a subject access request they must immediately forward it to the nominated contact named in section 5.2.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if they do not receive the additional information.

### **Requests Made by Third Parties or on Behalf of Children**

The Trust or schools need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney. The Trust or School may also require proof of identity in certain circumstances.

### **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 students at our school may not be granted without the express permission of the student. This is not a rule and a student'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. These include, but are not limited to: passport, driving licence, utility bills with the current address, birth / marriage certificate, P45/P60 and a credit card or mortgage statement
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Pertains to confidential references: The Trust or its schools do not have to disclose any confidential references given to, or received from, third parties for the purpose of actual or prospective:
  - education, training or employment of the individual;
  - appointment of the individual to any office; or
  - provision by the individual of any service
- is subject to legal professional privilege.
- relates to any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.
- consists of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

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

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

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the Trust or school will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

#### School Closure Periods

The Trust or schools may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the School will be closed and non-essential administration functions are suspended, we do not review emails during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the schools re-open. The Trust and its schools will endeavour to comply with requests as soon as possible and will maintain communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

#### **9.4 Other data protection rights of the individual**

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

#### **9.5 Employee Obligations**

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the schools in the course of their employment or engagement. If so, the Trust or its schools expects those employees to help meet our data protection obligations to those individuals. Specifically, you must:

- Only access the personal data that you have authority to access, and only for authorised purposes
- Only allow others to access personal data if they have appropriate authorisation
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction [Please refer to the School's eSafety, Cybersecurity, Information Security, Acceptable Policy and the School's information management toolkit for further details about our security processes])
- Not remove personal data or devices containing personal data from the Trust or school premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information
- Not store personal information on local drives

#### **10. Parental requests to see the educational record**

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

#### **11. CCTV**

We use CCTV in various locations around our school sites to ensure they remain safe. We adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. CCTV footage is retained for 30 days as deemed appropriate as per each school's CCTV usage policy.

## **12. Photographs and videos**

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

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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.

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.

## **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:

- 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 privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies, automated processing, large scale processing of special category data, or large scale monitoring of publicly accessible spaces (through the use of CCTV).

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## **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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops
- 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**

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. Disposal certificates will be obtained on the destruction of paper records and electronic equipment.

### **16. 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 the Data Breach Policy.

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

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

In case of suspected breach, contact the person designated as the key point of contact for personal data breaches in order to complete the data breach form. Further information can be found in the Data Breach Policy.

### **17. 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.

### **18. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

### **19. Links with other policies**

This data protection policy is linked to the following policies:

- CCTV

- Child protection and safeguarding
- Cybersecurity
- Data Breach
- E-safety
- Freedom of information
- Information Security
- Photography
- Social networking and media

The Governors have overall responsibility for the operation of this policy and it will be reviewed annually.