THE WESTGATE SCHOOL

Hampshire's First 4-16 'All Through' School

"The Westgate School is a community of learners where partnerships inspire success for all: learning together – achieving excellence"

Headteacher: Mrs F A Dean, MA (Ed)

Initial Policy date	May 2018	Next scheduled review	June 2025
Governor approved	June 2024	Key person/people	Senior Site & Facilities Strategic Lead
Model Policy	N/A	Model localised	Yes
Pupil leadership team review		~~Y / N / N/A~~	

DATA PROTECTION POLICY

Our aims are to:

Data Protection falls within the scope of the Data Protection Act (DPA) 2018, which sits alongside the General Data Protection Regulation (GDPR), and tailors how GDPR applies in the UK. This policy follows the recommendations issued by the Information Commissioner's Office In accordance with powers under the 2018 Act. This policy applies to all personal data, regardless of whether it is in paper or electronic format. It also applies to Transfer of data outside of UK or EEA, and automated processing/ profiling.

Contents.

21. Links with other policies

1. Legislation and guidance.

This policy meets the requirements of:

- 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 Protection of Freedoms Act 2012 when referring to our use of biometric data.
- It reflects the ICO's code of practice for the use of surveillance cameras and personal information.
- 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, 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

	• Criminal Records
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing by transmission, disseminating, or otherwise making available, alignment or combination, 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 organization 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.

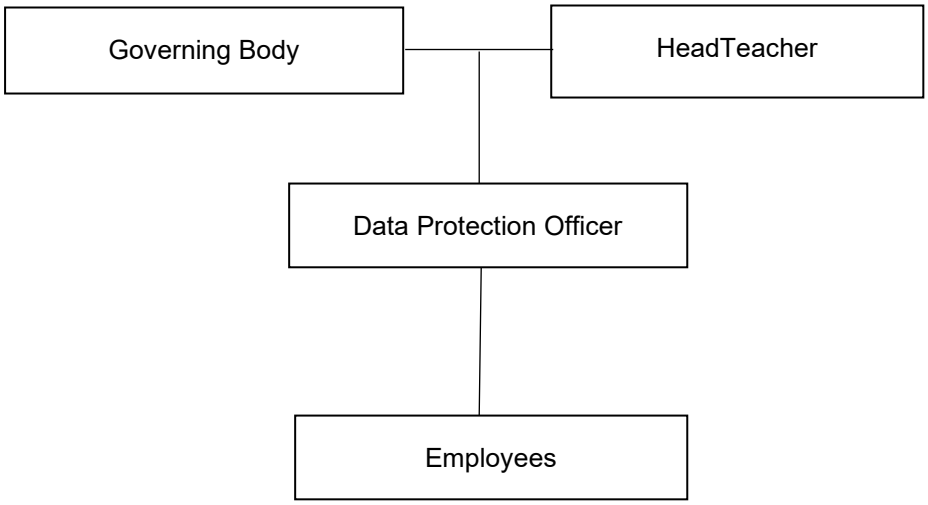
3. Data Controller.

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

The school is registered as a Controller with the Information Commissioner's Office (ICO) (Registration reference: ZA336960) and will review and renew this registration annually or as otherwise legally required.

4. Roles and responsibilities.

This policy applies to **all employees** at The Westgate School and day-care Nursery, volunteers and external organisations or individuals working on our behalf. Colleagues who do not comply with this policy may face disciplinary action, in accordance with the school (Model) Code of Conduct Policy. The following is the Data Protection organogram for The Westgate School:



4.1 Governing body.

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection laws and with demonstrating their accountability and commitment to these compliance obligations. All Governors are issued with individual school email accounts, which are to be used when dealing with school Data. The clerk of Governors is to arrange the necessary requirements as part the induction and end of tenure process.

4.2 Data Protection Officer (DPO).

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with applicable Data Protection law, and developing related policies and guidelines where appropriate.

They will provide a report of their activities directly to Governors Resources Committee and, where relevant, report to the Full Governing Body for 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 Senior Site & Facilities Strategic Lead is contactable via contact@westgate.hants.sch.uk.

4.3 Headteacher.

The headteacher acts as the representative for the school as a data controller, on a day-to-day basis.

4.4 All employees.

All colleagues 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

5. Data protection principles.

There are seven key principles under UK GDPR which our school must comply with.

The principles say that personal data must be:

- Fairly, lawfully, and transparently processed
- Processed for clear and limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary i.e. not excessive
- Accurate
- Kept for no longer than is necessary
- Secure, i.e. its integrity and confidentiality must be maintained

- Processed responsibly i.e. we must be able to demonstrate our accountability by keeping appropriate records to show how we comply with the other principles, and respect the individual's rights in relation to the data we process.

This policy sets out how the school aims to comply with these principles and applies to all personal data however it is collected, used, recorded, stored or in any other way processed by the school and whether it is held on paper or electronically.

6. Collecting personal data

6.1 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 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 one 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.

6.2 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.

Employees must only process personal data where it is necessary in order to complete their roles.

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

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

7. 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 employees 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 employees and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data processing or 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.
        - This must be signed at third party company director level, and approved by The Westgate School Data Protection Officer
    - 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
    - Carry out a **Data Protection Impact Assessment** (DPIA), where appropriate, to assess the risk to the individual.
    - DPIA to be carried out for the implementation of any software system – an example was a DPIA supported the implementation of EduLink One
        - Employees must seek authorisation from The Westgate School Data Protection Officer for the implementation of any new software packages

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

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

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

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

7.1 Restricted transfers.

UK GDPR restricts transfers of personal data to a separate organisation located outside of the UK, unless the rights of the individuals in respect of their personal data is protected in another way.

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:

- 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 colleagues receive a subject access request they must immediately forward it to the DPO.

8.2 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. (See point 9, however, for further details relating to this.)

Secondary Phase:

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

Each request should be considered and treated on a case by case basis. When responding to requests, we:

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

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers 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. 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.

8.4 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 6), 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 based on public interest
- Individuals have the right to be informed about the collection and use of their personal data 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. Parental requests to see the educational record

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.

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

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

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. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012. A DPIA will be completed for this processing where biometric authentication and recognition systems are used.

Parents/carers will be notified regarding our biometric recognition system. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners, by purchasing pre-payment cards from the main office, which can be swiped at the tills.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where employees members or other adults use the school's biometric system(s), we will also obtain their consent, and provide the alternative means mentioned above, if they object. Employees and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

11. CCTV

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

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

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

12. Photographs and videos

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

Primary Phase.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child 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.

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.

Secondary Phase.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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 pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, 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.

See our Child Protection Policy for more information on our use of photographs and videos.

13. Artificial intelligence (AI)

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

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

If personal and/or sensitive data is entered into an unauthorised generative AI tool The Westgate School will treat this as a data breach and will follow our personal data breach procedure.

14. Data protection by design and default

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

- A suitably qualified DPO, who will have the necessary resources to fulfil their duties and maintain their expert knowledge, has been appointed and notified to the ICO for inclusion in the public register entry for the school as Controller.
- 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
- Completing Data Protection Impact Assessments (DPIA) where the school's processing of personal data presents an elevated risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).
- Integrating data protection considerations into relevant internal documents such as policies and procedures related to this policy. Our Privacy notices, which will be displayed on the school website.
- Regularly training members of staff on data protection compliance, 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Control Access: Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, must be kept under lock and key when not in use
- Keep a Clear Workspace: Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Keep Track of Off-Site Personal Data Activity: Where personal data needs to be taken off site, i.e medical care plans, colleagues will need to sign for them in and out of the school
- Password Management: Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Employees and pupils should not reuse passwords from other sites
- Protect Devices: Encryption software used to protect all portable devices and removable media, such as laptops and USB devices
- Acceptable Use: Employees, pupils or governors who store personal data on their personal devices are expected to follow the same security procedures as for school-owned equipment in accordance with our online safety policy/ICT policy/acceptable use agreement/policy on acceptable use
- Third Party Risk Management: 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

16. Retention and disposal of records

We will only keep personal data for as long as necessary with respect to our processing activities as a school. We will follow [state what guidelines are followed as a school for retaining records etc.

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, in accordance with our Record of Processing Data (ROPA).

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use an approved 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.

To reduce the amount of data we hold in school email accounts, all emails are automatically deleted after an 18-month period.Our retention and disposal procedure is in accordance with the HCC School Records and Retention Schedule.

17. Personal data breaches

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

When appropriate, we will report the data breach to the ICO within 72 hours, we will follow the procedure set out in appendix three. 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

All individuals, who are obliged to follow this policy, are encouraged to report any suspicious activity or data security incident to the DPO so that it can be considered, investigated and the situation appropriately managed or reported.

17.1 Data breach near misses.

The Data Protection Officer will record data breach near misses following the same model for health and safety near misses.

18. Training.

Al employees and governors are provided with data protection eLearning training as part of their induction process.

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

19. Monitoring arrangements.

The DPO is responsible for monitoring and reviewing this policy and procedure. Major changes will be brought to the Governing body, if this is prior to this policy review.

This policy will be reviewed annually and approved by the full governing board.

20. Analytical cookies.

On accessing The Westgate School website, a ‘cookie’ (a small identifying text file) is automatically stored on the user’s computer in order to speed up access on future occasions. We need to use temporary cookies to maintain your user session and tell our server which page to pull up next, such cookies are allocated to your device only for the duration of your visit to this website and expire when you close down your browser. We also need to use traffic log cookies to measure which pages are being used and which ones aren’t; this helps us make improvements to the site and ensure its effectiveness.

We do not use cookies to store or collect personal information and therefore our use of cookies does not impact on your privacy. However, the Privacy and Electronic Communications (EC Directive) Regulations 2003 require website users to consent to the storage of access to cookies (unless they are strictly necessary to enable us to provide you with any service you have requested). By using the school website and online services you agree that we may place the cookies mentioned above on your device.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Safeguarding policies
- Retention
- School (Model) Code of Conduct Policy
- CCTV
- Online safety policy/ICT policy