



| | |
|------------------|----------|
| Sponsor | Bursar |
| Review Date | Sep 2022 |
| Next Review Date | Jan 2023 |
| Committee | Estates |

DATA PROTECTION POLICY

Data Protection Principles

The Data Protection Act 2018 incorporating the General Data Protection Regulations [GDPR] is based on data protection principles that our school must comply with.

The principles say that personal data must be:

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

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

Collecting Personal Data

Lawfulness, Fairness and Transparency. We will only process personal data where we have one of 5 '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 against identity theft or protect their reputation
- 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/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 which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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

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 Data Retention and Storage Policy.

Sharing Personal Data

We only share personal data with others to fulfil our contractual and legal obligations, if we have a legitimate interest as described in our Privacy Notice or we have gained explicit consent to do so. Examples of when we may share data are:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, catering contractors and travel 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
- The school may use a third party to gather information about individuals from publicly available sources – for example, Companies House, the Electoral Register and the media – to help understand more about the individual and their ability to support us.

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 situation 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 data protection law.

Who Does What

The Data Controller

Woldingham School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore Woldingham School is a data controller.

Woldingham School is registered as the data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and Responsibilities

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

Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations and has a nominated role responsible for Data Protection.

Privacy Officer

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

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

The PO is also the first point of contact for individuals whose data the school processes, and for the ICO. The PO is contactable via privacy@woldinghamschool.co.uk or 01883 654278. The Bursar acts as the representative of the data controller, and is the overall authority for Data Protection, on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the PO 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

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 Annex D.

Training

All staff and governors are required to undertake data protection training as part of their induction process and then to stay up to date with any changes to Data Protection law and school policies.

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

Links with other policies

This data protection policy supports our other policies including:

- Safeguarding and Child Protection policy
- ICT Acceptable Use (Staff) policy
- ICT Acceptable Use (Student) policy
- Admissions policy
- Data Retention and Storage policy
- Recruitment, Selection and Disclosure policy
- Security, Access, Workplace Safety and Lone Working policy

Annexes

- A. Legal Considerations
- B. Access to Information.
- C. Technical Considerations.

Annex A

Legal Considerations

Aims

Woldingham 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 [General Data Protection Regulation \(GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#). It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data. It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

Definitions

| Term | Definition |
|---------------|---|
| Personal data | Any information relating to an identified, or identifiable, individual. This may include the individual's: <ul style="list-style-type: none">• 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 | <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"> • 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 • Family Circumstances • Sex life or sexual orientation |
| Processing | Anything done to personal data (including photographic images and video), such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Data controller | A person or organisation that determines the purposes and the means of processing 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. |

Access to Information

Subject access requests and other rights of individuals

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

Subject access requests can be submitted electronically (email, website message or social media), verbally or in writing to the Privacy Officer [PO]. They should include:

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

If staff other than the PO receive a subject access request, they must immediately forward it to the PO with as much of the above information as possible.

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 13 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.

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one 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

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.

Other data protection rights of the individual

In addition to the right to make a subject access request (see paragraph 1.1), and to receive information when we are collecting their data about how we use and process it, 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 PO. If staff receive such a request, they must immediately forward it to the PO.

Parental requests to see the educational record

Parents, or those with parental responsibility, can request access to their child's educational record (which includes most information about a student) by applying in writing to the Deputy Head Academic.

There is no legal obligation to supply the educational record but we will, unless there are special circumstances, aim to respond with the data within 15 school days from the receipt of the request.

Technical Considerations

Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to register attendance), we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before their child first takes part in it. 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 students 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 students. For example, students can use a PIN code on the registration devices.

Parents/carers and students 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 student 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 student's parent(s)/carer(s).

CCTV

We use CCTV and Automatic Number Plate Recognition [ANPR] technology in various locations around the school site to ensure it remains safe. We will 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.

Any enquiries about the CCTV system should be directed to the PO. See also CCTV Policy.

Photographs and videos

In the normal day to day operation of the school we use photographic and video images of students and staff regularly, including to celebrate achievements at events and performances, provide a visual record of events and performances and to use in marketing materials.

Other uses may include:

- Internal identification purposes
- 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, including streaming of events.

Unless they have indicated to the contrary on the Form of Acceptance, parents' consent to the school making use of their daughter's photograph or image to feature in school communications and promotional materials whilst the girl is at the school and after she has left the school. 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. Parents who do not want their daughter's photograph or image to appear in any of the school's promotional material must make sure their daughter is also well aware of this fact.

In the case of media coverage where full names and images are required, the school will request parental permission to use imagery, full name and area of residence.

The school may use photography and video to record key school events in which images of parents may feature. These are disseminated to parents and alumnae and may be used for promotional purposes. Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the school expects all parents to follow:

- Parents should be mindful of the need to use their cameras with consideration and courtesy for cast members or performers on stage and the comfort of others.
- Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the school therefore asks that it is not used at indoor events.
- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
- Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
- Parents are reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts.
- Parents may not film or take photographs in changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.
- The school reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.
- The school sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase.

Use of cameras and filming equipment by pupils

All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of the pastoral staff. The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset. The misuse of images, cameras or filming equipment in a way that breaches this policy, or the Anti-Bullying Policy, or the Acceptable Use of Technology Policy, is always taken seriously, and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate.

See our Safeguarding and Child Protection policy, ICT Acceptable Use policies, Media Relations policy and the Social Media policy for more information on our use of photographs and videos.

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 Privacy Officer [PO], 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 Annex A)
- 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 (the PO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Annually 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*** – we will make available the name and contact details of our school and PO. We will also make available information about how we use and process their personal data (via our privacy notices)
 - ***For all personal data that we hold*** – we will maintain an internal record of the type of data we hold, who we hold that data about and how and why we are using the data. In addition, we will record any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

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. E.G. printed information used on school trips
- 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 and USB devices
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Information Security policy for further information)
- 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

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.