St David's College

— Est. 1965 —

DATA PROTECTION POLICY

School Community

UK Data Protection Law

Date	Review Date	Monitoring	Coordinator	Nominated Governor
01/09/2026	01/09/2027	**Annually by Fin com**	**A Goodwin**	**Adam Williams**

Data protection in the UK is governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), as amended by the Data (Use and Access) Act 2025 (DUAA 2025), together with other applicable legislation. The DUAA received Royal Assent on 19 June 2025. It amends the existing framework and does not replace the UK GDPR or the DPA 2018. This policy reflects the law and guidance in force at the date of its review.

Controller

St David's College complies with the UK GDPR and is registered as a fee payer with the Information Commissioner's Office (Reg. No. Z7540089).

The Data Protection Officer (DPO) for the school is Mr A Goodwin.

We ensure that your personal data is processed in accordance with the principles set out in article 5 of the UK GDPR, which are as follows:

1 **Lawfulness, fairness and transparency:** processing personal data in accordance with the prescribed lawful conditions set out at Articles 6 and 9 UK GDPR and Schedule 1 DPA, in addition to being transparent with individuals about

the processing undertaken and also fair in how personal data is used (Principle One).

2 **Purpose limitation**: the requirement to collect personal data for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes (Principle Two).

3 **Data minimisation**: the personal data collected and processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle Three).

4 **Accuracy**: collecting and processing personal data that is accurate and as necessary kept up to date (Principle Four).

5 **Storage limitation**: personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Principle Five).

6 **Integrity and confidentiality (security)**: personal data is processed in a manner that ensures appropriate security of the personal data, including protection against

unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Principle Six).

7 **Accountability**: complying with the UK GDPR and also being able to demonstrate your compliance through records kept and embedded knowledge of the law (Principle Seven).

Rights

The UK GDPR provides the following rights for Individuals over the processing of their personal data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

- *See the ICO website for more details about what these rights entitle you to know and be able to do with the personal data under our control https://ico.org.uk* https://ico.org.uk

Collecting and using pupil information

We collect and use pupil information under the principles set out above. Principle Two states that data is used for "specified, explicit and legitimate purposes". We collect and use pupil data to:

- Process admission and registration
- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Assess the quality of our services
- Comply with the law regarding data sharing
- The prevention and detection of crime
- Protecting vulnerable individuals
- Process any complaints

Pupil information which we collect, hold and share include:

- Personal information (i.e. name, unique pupil number and address)
- Characteristics (i.e. ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (i.e. sessions attended, number of absences and absence reasons)
- National curriculum assessment results
- Special educational needs information

- Relevant medical information
- Information about behaviour in and outside of the school
- Safeguarding information in accordance with the law and statutory guidance issued by the Welsh Government

When the School provides online services likely to be accessed by children, it will take account of children's rights and particular privacy needs. The School will use clear, age-appropriate privacy information and consider appropriate safeguards when designing or choosing services that process children's personal data.

Processing Information

We process pupil information for the following lawful reasons as prescribed under the UK GDPR or DPA:

- **Performing or taking steps to enter into a contract**: as a fee paying independent school, placements are governed by contracts with parents and local authorities which require certain information to be collected to enable the contract to be entered into and thereafter performed pursuant to the terms agreed.

- **Legal obligation**: there are various laws which apply to the operation of an independent school which require personal data to be processed about pupils, parents and others. These laws include the Independent School Standards 2024 for Wales, the National Minimum Standards for Boarding Schools (Wales) and various education acts passed by the Senedd and the United Kingdom Parliament (prior to devolution and which have not yet been repealed in Wales). This includes personal data relating to attendance, safeguarding, behaviour, special educational needs, managing medical conditions, health and safety reporting, progress in the curriculum and issuing reports to parents.

- **Vital interests**: we may need to act quickly and use the personal data we control in order to protect the vital interests of a pupil, parent or other. This may also include special categories of personal data[1] (SCPD) or criminal data that we hold about an individual.

- **Legitimate interests**: we may process personal data when we have identified a legitimate interest for the school or a third party. In doing so we will balance the legitimate interest of the school/third party against any potential impact on the rights and freedoms of an individual. This will primarily cover personal data we process which is not required to meet a legal requirement or to perform the placement contract.

[1] Special categories of personal data are: race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data, health, sex life and sexual orientation.

- Consent: only in limited circumstances will we seek to rely on your consent as an appropriate lawful basis to process personal data. For example, when processing personal data on our website in the form of images or other materials used for public circulation. In seeking consent we will ensure that you are provided with enough information so that you are informed before giving your consent and clear on the specific purpose for which your consent is sought. You have a legal right to withdraw your consent at any time.

- **Substantial public interest**: we process SCPD under this condition when there is a further, more specific, condition set out under Schedule 1 of the DPA. This includes when SCPD is processed to safeguard pupils, to prevent or detect unlawful acts, supporting individuals with medical conditions or disabilities or insurance arrangements.

Storing pupil data

We hold pupil data on their educational record for 25 years after leaving school or for the duration directed by law. After this point the data will be anonymised in line with best practices and used only for statistical and research purposes or erased entirely.

With permission or request, personal data will be stored for students who become a member of the Old Davideans' Association (ODA). This will include; name, address, Telephone number, email address. Information will be accessible by the Headmaster and Headmaster's secretary for the purpose of informing parents and students of the ODA. Personal information is not shared with the ODA. Refer to the ODA data privacy policy for details on how they collect and transfer data.

Communication and our school community

In order to establish effective communication and partnership with parents and our school community we aim to provide an open and communicative environment forming a link between the classroom and the home, and the school and the family.

Our methods of communication include:

Letters
Texts
Phone Call
Email
Teams

We also use the following social media sites:

X
Facebook
WhatsApp
Instagram

Information about how these social media platforms may process your personal data can be found in each platform's respective privacy notices.

Admissions

As part of the registration and admissions process, personal and sensitive data will be collected. Information is retained for a maximum period of 6 months for those applicants who are not successful. For those who do not take up their place at St David's College but register further interest for the future, email addresses will be added to the emailing list within admissions and marketing and kept for a period of 3 years. Parents who wish to remove details should follow our guidance on 'rights for erasure'.

Photographs

The School may take photographs, videos or webcam recordings of pupils or students for official educational purposes or internal management.

- Admission/Application
- MIS system,
- Lesson observations/monitoring
- Other internal educational purposes
- Safety / pupil & School protection (CCTV)

Photographs may also be taken for external purposes that may be viewed by the general public. These include:

- Ceremonies
- Newspaper articles
- Marketing brochures
- Website articles
- School X page
- School Snapchat
- Official School Facebook account

If you do not wish to have photographs/ videos taken of yourself (student) or of your child (Parent) that may be viewed by the general public please ensure that the appropriate box has been ticked on our data protection compliance form to confirm that you do not consent.

On leaving the school, photographs and videos may be used for marketing purposes unless you provide us with notice that you wish to withdraw your consent. You may also complete a 'right of erasure form' if you wish the photograph(s) or video(s) to be deleted.

Biometrics

The school operates biometric recognition systems (fingerprinting) to allow entry into some areas of the school

All data collected will be processed in accordance with the UK GDPR, DPA and the Protection of Freedoms Act 2012.

The consent of at least one parent will be obtained before biometric data is taken and used. If one parent objects in writing, then the school will not take or use a child's biometric data. The pupil's consent will also be obtained.

For more information about biometric data please refer to the ICO Guidance.

Sharing Information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We routinely and/or occasionally share pupil information with:

- Estyn
- NHS (vaccinations/school nursing service)
- Progresso Management system
- Police, Fire, Rescue, Ambulance services
- Social Services
- CAMHS
- Other schools/academies/MATs (during pupil transfer)
- Examination boards (JCQ – access arrangements online, Edexcel, Cambridge, OCR, WJEC, AQA.)
- Offsite learning providers
- Residential trip organisers (and insurers)
- Bentley Photographic (school photographers)
- Sixth form colleges & other post-16 providers
- Medical centre

• Local Authorities

Processors

We use third parties to process personal data on the School's behalf, including IT platforms and other service providers. Where a provider acts as a processor, the School puts in place a written contract requiring it to process personal data only on the School's instructions and to apply appropriate technical and organisational security measures.

Aged 14+ Qualifications

For pupils enrolling for post-14 qualifications, the Learning Records Service will give us a pupil's unique learner number (ULN) and may also give us details about the pupil's learning or qualifications.

Artificial intelligence and digital services

How the School uses AI

The School may use approved digital services, including artificial intelligence (AI), to support teaching, learning and administration. These may include AI features within other services and tools made available to pupils. Before a service is used, the School considers its purpose, the personal information involved, how the provider handles that information and the safeguards required. Staff follow separate School procedures for selecting, approving and developing these services.

Personal information and safeguards

The School does not permit staff to enter identifiable information about pupils, families or staff into public or unapproved AI tools. An AI service may process personal information only where the School has specifically approved that use and put appropriate safeguards in place. The School checks how a provider handles information submitted to its service, including whether it may be used to train or improve AI models, how long it is kept, who can access it and whether it is shared.

Human oversight and pupils' rights

AI outputs may be inaccurate, incomplete or biased. A member of staff checks them before the School relies on or shares them. AI does not replace professional judgement, safeguarding practice or appropriate human engagement with a pupil or family. The School will not make a decision with a legal or similarly significant effect solely through automated processing unless data protection law permits it and the required safeguards are in place.

When choosing online services that pupils may use, the School considers their age, understanding, privacy, accessibility and safeguarding needs. Pupils and parents can use the rights and complaints routes in this policy to ask questions or raise concerns about personal information processed through an AI-enabled service.

Requesting access to your personal data

Under the UK GDPR, individuals have the right to request access to the personal data the School holds about them. To make a subject access request (SAR), or to request access to a child's educational record where applicable, email or write to the Headmaster, Mr Andrew Russell, describing the information requested. The School will respond without undue delay and normally within one month. The response period may be extended where the law permits, including by up to a further two months for a complex request or where the School receives a number of requests. If the School reasonably needs clarification to respond to a SAR, it may ask the requester for clarification; the response time limit is paused from the date clarification is requested until the School receives it. The School will explain any extension or pause and keep the requester informed. For more information about individual rights, see the ICO website at https://ico.org.uk.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed

Complain to the School's Data Protection Officer or the Information Commissioner's Office (ICO).

- Claim compensation for damages caused by a breach of the Data Protection Regulations

Security Measures

How do we look after your personal data and keep it safe?

Access to your personal data will be limited to school staff who need to know about you.

Information held on paper files are securely stored at the school and information stored on computer will be held securely behind passwords and other measures.

Information held on electronic files may also be stored for the school on 'cloud-based' servers providing that we are satisfied that our personal data will be held securely and protected from any unauthorised access.

We work in conjunction with our IT partners to ensure that computers and servers comply with all up to date Government regulations and are secure with:

- anti-virus software
- fire wall software
- passwords

All school personnel are trained to:

- be discreet and confidential
- consider the safe and secure positioning of computers
- back up data
- turn off computers when not in use
- remember password access
- lock filing cabinets and doors to offices
- shred confidential material
- clear their desk before they leave school

Right to Erasure

You have the right to request the deletion of your data where there is no compelling reason for its continued use. See 'collecting and using data' for details on legal duty. Parents

should fill a ‘Right to Erasure’ request form and send it to the Headmaster, Mr Andrew Russell. A verbal request may be made directly to the Headmaster. A meeting with the headmaster may be required in order to support the request. Where pupils have made a request, parents will be informed followed by a meeting with the Headmaster. The school will ensure that all data requests are completed within one month.

Equality

Under the Equality Act 2010, St. David’s has a duty not to discriminate against any of the protected characteristics. Due regard has been given to equality law when developing and implementing St David’s policies, practices and day-to-day activities. St David’s will continually monitor the way this policy operates to ensure it does not unlawfully discriminate, permit harassment or victimisation, or limit equality of opportunity. St David’s is committed to meeting its obligations under the Equality Act 2010 at all times.

Data protection complaints and contact information

If you are concerned about how the School uses your personal data, you can contact the Data Protection Officer (DPO), Mr A Goodwin, by email at agoodwin@stdavidscollege.co.uk or by writing to the School. We will acknowledge your complaint within 30 days, investigate it appropriately and tell you the outcome. You may also raise a concern with the Information Commissioner's Office (ICO) at https://ico.org.uk/concerns/.