

ST DOMINIC'S GRAMMAR SCHOOL

WEBSITE PRIVACY AND COOKIES NOTICE

Academic Year 2026–2027

Plain-language summary. We use website information to operate and secure the site, respond to enquiries, manage requested services and—only where permitted—communicate about the School. We do not sell personal information. Optional cookies and tracking technologies are not activated before a valid choice is made.

Notice control	Approved position
Website	www.stdominicsgrammarschool.co.uk
Who this covers	Website visitors and people who use online forms or website-linked services, including prospective/current families, pupils, applicants and members of the public
Data controller	St Dominic's Grammar School, acting through its Proprietor, Mr Gary Hartland
Operational lead	Sharon Tillett, Operational Data Protection Lead – stillet@sdgschool.co.uk
School address	Bargate Street, Brewwood, South Staffordshire, ST19 9BA
Telephone	01902 850248
Approval date	30 August 2026
Effective date	1 September 2026
Next review	By 31 August 2027 and whenever website processing, cookies, forms, suppliers or law materially change
Publication	Website footer and beside relevant online forms; cookie settings available from every page
Version	1.0 – complete replacement of the former website privacy statement

1. Why this separate notice is needed

The Data Protection and UK GDPR Policy explains the School's governance and operating rules. The Online Safety, Acceptable Use and Data Security Policy governs safe use of technology. Neither document, by itself, gives website visitors all the information required at the point their information is collected or explains cookies and similar technologies. This notice supplies that public transparency layer and should be read with any shorter notice displayed on a specific form.

This notice applies to the School's public website and online forms or services linked from it where the School determines why and how personal data is used. Separate notices may apply once a person becomes an applicant, pupil, parent, employee, volunteer, governor, contractor or alumnus; those more specific notices take precedence for that processing.

2. Legal framework and principles

- UK General Data Protection Regulation (UK GDPR), as amended.
- Data Protection Act 2018.
- Data (Use and Access) Act 2025 (DUAA), including provisions in force from 2026.
- Privacy and Electronic Communications Regulations 2003 (PECR).
- Human Rights Act 1998 and Equality Act 2010.
- Keeping Children Safe in Education 2026, where website information raises safeguarding concerns.
- DfE data-protection-in-schools guidance updated in 2026 and ICO guidance on transparency, children, direct marketing, cookies and online tracking.
- Current Independent School Standards and ISI leadership-and-governance expectations.

We process personal information lawfully, fairly and transparently; for specified purposes; in the minimum necessary amount; accurately; no longer than needed; and with appropriate security. We document decisions and review website suppliers, forms and tracking before use.

3. Information we collect

Information you provide

- name, title, relationship to a child and contact details;
- information in contact, prospectus, tour, open-event, admissions or general-enquiry forms;
- a child's name, age/year group, proposed entry point and educational interests where relevant to an enquiry;
- event, newsletter, alumni, fundraising or community preferences where those services are offered;
- recruitment or vacancy-enquiry information submitted through a website route;
- messages, attachments, questions, complaints, feedback and consent/preferences;
- accessibility or communication needs voluntarily supplied;
- information provided during a telephone call made using details displayed on the site; calls may be recorded for training and monitoring where callers are informed.

Information collected automatically

- internet protocol (IP) address, approximate location, browser, device and operating-system information;
- date/time, pages viewed, referring page, link interactions, session and error information;
- security, bot-detection, rate-limiting, load-balancing and consent-preference records;
- cookie or similar-technology identifiers where used;
- analytics information where the visitor has consented or another PECR exemption lawfully applies.

We do not intentionally collect special-category or criminal-offence data through ordinary website forms. If a person includes health, SEND, safeguarding, ethnicity, religion or other sensitive information in a message, it is handled only where necessary under the appropriate additional legal condition and transferred promptly to the correct secure School process.

4. Sources of information

Information comes mainly from the visitor, their browser/device and the School's website or form providers. It may also come from a parent/carer or authorised representative; an existing School record where linking an enquiry is necessary; fraud/cyber-security services; social-media or event platforms when a person deliberately interacts with the School there; and publicly available sources where verification or safeguarding makes this necessary and lawful.

5. Why we use website information and lawful bases

Purpose	Likely lawful basis
Operate, secure, diagnose and maintain the website; prevent abuse and preserve evidence	Legitimate interests in secure, reliable services; legal obligation where applicable. Strictly necessary technologies rely on the PECR exemption.
Answer a general enquiry, supply a requested prospectus or arrange a visit	Legitimate interests; steps requested before entering a contract where the enquiry concerns admission or services.
Manage admission, nursery, event, club or other requested service interest	Pre-contract steps; contract where applicable; legitimate interests; legal obligation for later formal processing.
Handle safeguarding, welfare or emergency information	Legal obligation, vital interests and/or legitimate interests; an Article 9/Data Protection Act condition where sensitive data is involved.
Recruitment enquiries and vacancy applications	Pre-contract steps, legal obligation and legitimate interests; the Recruitment Privacy Notice then applies.
Send electronic news, event or promotional communications	Consent where PECR requires it; permitted existing-relationship route only where applicable, with an easy opt-out; underlying processing recorded.
Optional analytics, embedded media or preference features	Consent under PECR before storage/access on the device, plus consent or legitimate interests for subsequent processing as appropriate.
Establish, exercise or defend legal claims and handle complaints	Legitimate interests and legal obligation; legal-claims condition where special-category data is necessary.

Consent is not bundled with access to the website and may be withdrawn as easily as it is given. Withdrawal does not affect processing already carried out lawfully. We do not rely on "public task" as a general basis for operating an independent-school website.

6. Children and safeguarding

- The website is designed for families and may be visited by children. Information is written as clearly as practicable and a child can ask an adult or the School for help.
- A child should not use a public form to send detailed medical, safeguarding, identification or financial documents unless specifically directed to a secure process.
- Where an online service is offered directly to a child and relies on consent, the School assesses competence and the UK parental-authorisation requirements for children under 13.
- Information indicating risk of harm is shared promptly with the DSL or emergency/safeguarding services as necessary. Data-protection law does not prevent proportionate safeguarding action.
- Do not use a routine website form for an emergency. Call 999 where there is immediate danger and use the School's published safeguarding route for urgent School concerns.

7. Who we share information with

Access is limited to people who need the information. Depending on the enquiry and service, recipients may include authorised School staff and the Proprietor; website hosting, maintenance, security, email, form, consent-management and IT providers; admissions, events, recruitment, payment or communications providers; professional advisers, insurers and auditors; and police, local authorities, safeguarding partners, regulators or courts where required or permitted by law.

Processors act under written terms requiring confidentiality, security, assistance, deletion/return and sub-processor controls. A supplier is not permitted to use School information for its own advertising or unrelated profiling. Where an external site or platform is an independent controller, its own notice also applies.

8. Third-party links and embedded content

- The site may link to social media, video, maps, ticketing, payment, recruitment or other external services. Following a link takes the visitor to another controller whose privacy notice should be read.
- Embedded videos, maps, feeds, fonts, CAPTCHA or social-media features can disclose IP/device information and set third-party technologies. Non-essential content is blocked or privacy-enhanced until consent where required.
- A visible social-media link is not, by itself, permission for the platform to track a visitor before they choose to follow it.
- The School reviews embeds and plugins for necessity, age appropriateness, security, data location, retention, tracking and alternatives.

9. Cookies and similar technologies

A cookie is a small file stored on a browser or device. Similar rules can apply to pixels, tags, local storage, software development kits and device fingerprinting. The School must tell visitors what is used, what it does and why. Except where a technology is strictly necessary to provide a service requested by the visitor or transmit a communication, it is not set or accessed until valid consent has been given.

Category	Purpose and choice
Strictly necessary	Security, fraud/bot protection, network/load balancing, form submission, session continuity, accessibility and recording cookie choices. Always active only where genuinely essential; still explained.
Preferences / functionality	Remember optional display, language, media or convenience choices. Off by default where consent is required.
Analytics / performance	Understand visits, errors and site performance so the site can be improved. Off until consent unless a specific lawful PECR exemption clearly applies and is documented.
Embedded media / social	Enable external video, maps, feeds or sharing functions that may contact a third party. Blocked until consent where not strictly necessary.
Advertising / profiling	Measure or target advertising across services. The School does not permit these without explicit approval, DPIA/contract review, clear information and prior consent; they should normally be avoided on a school website.

10. Cookie banner and live cookie register

- “Accept all” and “Reject non-essential” must be equally clear and accessible at the first layer; no pre-ticked optional categories or misleading design.
- Non-essential scripts, pixels and embeds must remain blocked until the relevant positive choice. Continuing to browse is not consent.
- Visitors can reopen cookie settings from every page, change or withdraw choices at any time and use the site’s core functions after rejection.

- The live register states each cookie/technology name, provider, purpose, category, first/third party status and expiry/duration.
- Consent records are retained only as long as needed to demonstrate the choice and refreshed when purposes/technologies change or at an appropriate interval.
- The website is rescanned after plugins, embeds, marketing tools, hosting or design changes and at least termly; discrepancies are corrected promptly.

11. Direct marketing and communications

- Marketing choices are separate from a service or admissions enquiry and refusal does not disadvantage the person.
- Each electronic marketing message identifies the School and provides a simple unsubscribe route.
- The School keeps a minimal suppression record so a person who opts out is not inadvertently re-added.
- Service, safeguarding, admissions-process or contractual messages are not treated as marketing merely because they are sent electronically.
- Purchased, scraped or unlawfully shared marketing lists are not used. Social-media custom audiences or tracking pixels require explicit senior approval, documented legal assessment and prior consent where applicable.

12. International transfers

Some website, email, security, analytics or embedded-content providers may process information outside the UK. The School uses them only where a UK adequacy regulation, UK International Data Transfer Agreement/addendum, binding corporate rules, permitted derogation or other lawful safeguard applies. Required transfer risk/data-protection assessments and supplementary measures are documented. Visitors may request information about material safeguards.

13. Retention

Information	Normal approach
Unsubmitted form data	Not intentionally retained by the School; provider/security logs may exist for a short technical period.
General website enquiry	Normally up to 24 months after the last meaningful contact, unless it becomes part of an admissions, complaint, safeguarding, contractual or legal record.
Prospectus, visit, open-event or admissions interest	Transferred to the admissions record and retained under the relevant privacy notice and Records Retention Schedule.
Marketing preferences	Until withdrawal or the service ends; suppression information retained minimally to honour opt-out.
Recruitment information	Managed under the Recruitment Privacy Notice and recruitment retention schedule.
Security/server logs	For the shortest period consistent with investigation, security, continuity and legal needs; normally no longer than 12 months unless an incident/legal hold requires longer.
Cookie/consent and analytics data	The exact cookie duration appears in the live register; consent proof and analytics are retained only for a documented, proportionate period.

Safeguarding, complaint, legal claim, insurer or regulatory requirements can justify longer retention. At expiry, information is securely deleted, destroyed or irreversibly anonymised. Backups expire through controlled rotation and are not used as indefinite archives.

14. Security

- encrypted transmission (HTTPS), secure hosting, patching, malware and vulnerability controls;
- access limited by role, strong authentication and prompt removal when access is no longer needed;
- spam, bot, CAPTCHA/rate-limiting and monitoring controls proportionate to risk and privacy;
- secure routing of forms to approved School accounts/systems rather than uncontrolled inboxes;
- supplier due diligence, processor terms, backup/recovery and incident-response arrangements;
- regular testing of forms, permissions, retention, plugins and public exposure.

No internet transmission is entirely risk-free. Visitors should avoid placing unnecessary sensitive information in free-text fields and should use a secure method when the School requests documents. Suspected website or personal-data breaches should be reported promptly to the Data Protection Lead.

15. Automated decisions and profiling

The public website does not make solely automated decisions that produce legal or similarly significant effects about visitors. Security tools may automatically identify likely bots, spam or malicious activity, but material decisions are reviewable. If significant automated decision-making or profiling is introduced, the School will complete the required assessment, update this notice and provide the safeguards and right to contest required by law.

16. Your data-protection rights

Depending on the circumstances, a person may have rights to be informed; access; correction; erasure; restriction; objection; portability; withdrawal of consent; and safeguards concerning qualifying automated decisions. Rights are not absolute and lawful exemptions may apply.

Send a request to Sharon Tillett at stillet@sdschool.co.uk or to the School address. We may verify identity and authority proportionately. We respond without undue delay and normally within one month, subject to lawful clarification, extension, fee, refusal or exemption. A parent does not automatically own a child's personal data; competence, wishes, best interests and confidentiality are considered.

17. Questions and complaints

Questions or complaints should be sent to Sharon Tillett, Operational Data Protection Lead, at stillet@sdschool.co.uk, telephone 01902 850248, or St Dominic's Grammar School, Bargate Street, Brewood, South Staffordshire, ST19 9BA. The School investigates objectively and explains the outcome and any remedy. A person may also complain to the Information Commissioner's Office at ico.org.uk or 0303 123 1113.

18. Changes to this notice

The School reviews this notice at least annually and when forms, purposes, cookies, embedded content, suppliers, international transfers or law change. The website displays the current version and effective date. Material changes are highlighted appropriately; fresh consent is obtained where a new or changed non-essential cookie purpose requires it. Previous versions are retained for accountability.

19. Governance and implementation assurance

Owner	Required evidence
Website owner / provider	Current site map, form inventory, script/plugin list, live cookie scan/register, HTTPS/security maintenance, retention/deletion and change notifications.
Data Protection Lead	ROPA entry, lawful bases, privacy wording at collection, processor/transfer checks, DPIA screening, complaints/rights/breach records and annual review.
DSL	Safe routing and handling of website safeguarding content; child-friendly reporting information; no public exposure of sensitive pupil data.

Owner	Required evidence
Headmaster	Approval of material processing, embeds, analytics/marketing tools and risk actions; resource and accountability.
Proprietor/Governing Body	Annual assurance and challenge on transparency, cookies, suppliers, security, incidents and overdue actions.

Related School documents include the Data Protection and UK GDPR Policy; Online Safety, Acceptable Use and Data Security Policy; audience-specific privacy notices; Records Retention Schedule; breach and rights-request procedures; and Safeguarding and Child Protection Policy.