Charitable Objects of St. Catherine's School- *The Objects for which the Company is established are to promote and provide for the advancement of education by providing, conducting, governing, carrying on and maintaining in the United Kingdom, or elsewhere, a boarding or day School or Schools for girls in which the teaching shall be in accordance with the principles of the Church of England.*

ST CATHERINE'S SCHOOL BRAMLEY

DATA PROTECTION POLICY

'Believe… Achieve… Succeed'

Policy Holder	Caroline Mead
Date Approved	October 2026
Approval	Governance and Risk Committee
Date for next review	October 2027

This policy is reviewed annually or following significant changes in statutory guidance in the School's processing or following a significant data protection incident.

The Policy

This Policy replaces the Confidentiality and Privacy Policy, which is withdrawn with effect from the date of approval of this Policy.

Data protection is an important legal compliance issue for the School. In the course of its activities the School collects, stores and processes personal data about pupils, parents, staff, governors, applicants, alumnae, suppliers and others, and it needs to do so in order to operate, to educate and to safeguard.

This Policy sets out how the School meets its obligations under UK data protection law, and what it expects of those who handle personal data on its behalf. It is a single document serving two purposes: it is the practical standard that staff are required to work to, and it is the School's public statement of how it complies.

This Policy is not a privacy notice. Privacy notices are separate documents which tell individuals what the School does with their personal data, and they are a distinct legal requirement under Articles 13 and 14 of the UK GDPR. The School's privacy notices are listed in section 22 of this policy.

UK data protection law consists primarily of the UK General Data Protection Regulation (the "UK GDPR") and the Data Protection Act 2018, as amended, including by the Data (Use and Access) Act 2025 (together, "Data Protection Legislation").

1. Who this Policy Applies to

This Policy applies to all personal data the School processes, however it is held and wherever it is held.

Those who handle personal data as employees or governors of the School are required to comply with this Policy when doing so. A deliberate or negligent breach of this Policy may be treated as a disciplinary matter.

This Policy also represents the standard of compliance the School expects of those who handle its personal data as contractors, agency staff, peripatetic staff, volunteers, work experience students and gap year placement students, whether or not they are employed by the School.

Where the School shares personal data with third parties who are controllers in their own right (which may range from other schools, to parents, to public authorities) each party is separately responsible for its own compliance.

2. Definitions

Term	Meaning
Personal data	Any information relating to a living individual (a "data subject") by which that individual may be identified, whether directly or indirectly. It covers facts about an individual, including biographical and contact information; opinions and professional judgements, such as those recorded in school reports; and records of the School's or others' intentions towards an individual.
Processing	Virtually anything done with personal data, including obtaining or collecting it, recording it, structuring it, analysing it, storing it, sharing it internally or with third parties, and deleting or destroying it.
Controller	A person or body that determines the purposes and means of the processing of personal data, and which is legally responsible for how it does so. The School is a controller in respect of the personal data described in this Policy.
Processor	An organisation that processes personal data on behalf of a controller — for example a payroll provider, a cloud storage provider or a management information system supplier.
Special category data	The categories of particularly sensitive personal data listed at Article 9 of the UK GDPR.
Criminal offence data	Personal data relating to criminal convictions and offences, or to alleged offences and related proceedings, as described at Article 10 of the UK GDPR.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data.

3. Responsibility for Data Protection at the School

The School has appointed **Caroline Mead as its Data Protection Officer (DPO)**. The DPO has responsibility for overseeing the School's compliance with Data Protection Legislation, for advising the School on its obligations, and for acting as the point of contact for individuals and for the Information Commissioner's Office.

The DPO reports to the Heads and to the Finance and Risk Committee. The DPO's role in respect of data protection is independent: she is not instructed on how to carry out her data protection tasks, and she holds

no operational role which would place her in a conflict of interest in respect of the personal data the School processes.

Contact details for the DPO are at section 21 of this Policy.

Responsibility for compliance in day-to-day practice, rests with all staff. Those with management or leadership responsibilities are expected to champion the standards in this Policy within their areas and to ensure that concerns and incidents are reported promptly.

4. The Data Protection Principles

Article 5(1) of the UK GDPR sets out six principles which the School must comply with. Personal data must be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes;
3. adequate, relevant and limited to what is necessary for the purposes for which it is processed;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which it is processed; and
6. 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.

The School will, so far as is reasonably practicable, comply with each of these principles in all of its processing.

5. Accountability

Article 5(2) of the UK GDPR adds a seventh, overarching obligation: the School must not only comply with the principles but must be able to demonstrate that it does so. This is the accountability principle, and it is the reason the School maintains the documents and records listed below.

- A Record of Processing Activities, describing the personal data the School processes, why, on what lawful basis, with whom it is shared and for how long it is kept.
- Written agreements with its processors, and a register recording those agreements and the checks carried out on them.
- Data Protection Impact Assessments (DPIA), documenting significant decisions and risk assessments about new or higher-risk processing.
- A register of personal data breaches, including those which were assessed as not requiring notification and the reasons for that assessment.
- A log of subject access and other rights requests, and how they were handled.
- Records of staff data protection training.
- An Appropriate Policy Document, as required where the School processes special category and criminal offence data under certain conditions.
- An audit trail of when and how this Policy and the School's Privacy Notices were updated and communicated.

6. Personal Data the School Processes

The School may process a wide range of personal data about pupils, parents, staff and others as part of its day-to-day operations and responsibilities. This may include but is not limited to: names and addresses; contact details; bank details; nationality and other immigration status information; donation history; academic, disciplinary, admissions, safeguarding, pastoral, medical and attendance records; confidential references; examination scripts and pupils' marks; CCTV footage; and information held in electronic communications.

Further detail is given in the School's Privacy Notices and in its Record of Processing Activities.

Special category data

From time to time the School is required to process more sensitive personal data. Special category data is defined at Article 9 of the UK GDPR as personal data revealing or concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data, where processed for the purpose of uniquely identifying an individual;
- health;
- sex life; or
- sexual orientation.

The School also processes criminal offence data, principally in order to carry out vetting checks on those working or volunteering at the School.

The School will process such data in accordance with the rights or duties imposed on it by law, including as regards safeguarding, or from time to time on the basis of explicit consent where that is required. The reasons will include:

- to safeguard pupils' welfare and provide appropriate pastoral and, where necessary, medical care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of a pupil's health or medical condition or other relevant information where it is in her interests to do so. For example for emergency medical care, to arrange the assessment and diagnosis of health and medical conditions and special educational needs, for social protection, safeguarding, and cooperation with the police or social services, for insurance purposes, or to caterers or organisers of school trips who need to be made aware of dietary or medical needs;
- to comply with public health requirements;
- to provide educational services in the context of making reasonable adjustments for a pupil's disability or any special educational needs;
- to provide spiritual education in the context of any religious beliefs;
- as part of any School or external complaints, disciplinary or investigation process that involves such data, for example where there are special educational needs, health or safeguarding elements; and

- for legal and regulatory purposes, e.g. child protection, diversity monitoring, health and safety, and immigration and visa sponsorship compliance. To comply with the School's legal obligations and duties of care.

The specific conditions in Schedule 1 to the Data Protection Act 2018 on which the School relies, and the safeguards it applies, are set out in its Appropriate Policy Document.

7. Lawful Grounds for Processing

The School must have a lawful ground under Article 6 of the UK GDPR for every activity involving personal data. Consent is one such ground. However, given the relatively high threshold that consent must meet under Data Protection Legislation; it must be freely given, specific, informed, unambiguous and capable of being withdrawn. The School does not rely on consent for most of its processing.

In most cases, where the processing is necessary for the School in the ordinary and legitimate course of its running, including in order to meet its obligations to staff, pupils and parents, the School relies on one of the following grounds instead:

- **Contractual necessity** - the processing is necessary to perform a contract with the individual, or to take steps at their request before entering into one, for example under the Parent Contract or a contract of employment.
- **Legal obligation** - the processing is necessary for the School to comply with the law.
- **Vital interests** - the processing is necessary to protect someone's life.
- **Recognised legitimate interests** - the processing is necessary for one of the purposes pre-approved in Data Protection Legislation, which include safeguarding children and individuals at risk.
- **Legitimate interests** - the processing is necessary for the School's legitimate interests, or those of a third party, provided those interests are not outweighed by the impact on the individual. This is the most flexible ground but in most cases it requires a balancing exercise to be carried out and recorded.

Where the School does rely on consent, it will make that clear at the point the data is collected, and the individual may withdraw their consent at any time. Withdrawal does not affect the lawfulness of processing carried out before it.

8. Headline Responsibilities of all Staff

Record-keeping
It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue, or if they are dissatisfied with the accuracy or fairness of any personal data about themselves.

Staff should be aware of the rights set out in this Policy. Individuals about whom information is recorded on School business (notably in emails, notes and reports) may have the right to see that information. Staff should record information about pupils, parents, colleagues and others fairly, professionally and with restraint, and on the working assumption that the individual concerned may one day read it.

Data handling
All staff have a responsibility to handle the personal data they come into contact with fairly, lawfully, responsibly and securely, and in accordance with the School's policies and procedures, in particular the Information Security Policy and the Information and Communications Technology (ICT) Policy.

Responsible processing extends to the creation and generation of new personal data and records, which should always be done fairly, lawfully, responsibly and securely.

Reporting personal data breaches
Data Protection Legislation requires the School to report certain personal data breaches to the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to individuals' rights and freedoms, the School must also notify those individuals.

Every member of staff must therefore report any actual or suspected personal data breach immediately, and in any event on the same working day, to the Data Protection Officer and to the IT Support Department. This includes near misses and incidents which appear minor.

The decision whether a breach must be reported to the ICO, or to affected individuals, is made by the Data Protection Officer. Individual members of staff must not make reports to the ICO themselves.

An honest mistake reported promptly will not normally be treated as a disciplinary matter. A failure to report may be, because it exposes the School and the individuals concerned to significantly greater harm.

The most common cause of personal data breaches at the School, by a considerable margin, is email misdirection - sending information to the wrong recipient, or attaching the wrong document. Staff should check recipients and attachments before sending, take particular care with distribution lists and with automatic address completion, and pay close attention to any warning the email system displays about external recipients.

Full detail is documented in the School's Data Breach Policy.

9. Rights of Individuals

Individuals whose personal data the School holds have the following rights:

- to obtain access to, and copies of, the personal data the School holds about them;
- to require the School to correct the personal data it holds about them if it is inaccurate;
- to require the School, in certain circumstances, to erase their personal data;
- to request that the School restricts its data processing activities;
- to receive from the School, in certain circumstances, the personal data it holds about them which they have provided to the School, in a reasonable format specified by them, including for the purpose of transmitting it to another controller;
- to object, on grounds relating to their particular situation, to any of the School's particular processing activities where the individual feels this has a disproportionate impact on their rights;
- to object to direct marketing;
- to withdraw their consent, where the School is relying on consent to process their personal data, without affecting the lawfulness of processing carried out before withdrawal;
- to contest, or to seek human intervention in respect of, a decision made about them based solely on automated processing where that decision has a significant effect; and

- to complain to the School about how their personal data has been handled, and to complain to the ICO.

These rights are not absolute, and the School may be entitled to refuse a request where an exception or exemption applies. The School will respond to any such request as soon as is reasonably practicable and in any event within statutory time limits, which are generally one month. Where a request is complex, or where several requests are made, the School may extend that period by up to two further months and will tell the individual within the first month if it needs to do so.

Where the School needs clarification in order to identify the personal data sought, the time limit may be paused until that clarification is received. The School is required to carry out a reasonable and proportionate search, not an exhaustive one.

Any member of staff who receives a request from an individual seeking to exercise one or more of these rights or making a complaint about the handling of personal data, must forward it to the DPO immediately. A request does not have to use any particular form of words, or mention data protection at all, to be a valid request. The School's Subject Access Request Procedure sets out how such requests are handled.

10. Whose Rights - Pupils, Parents and Children's Data

The rights under Data Protection Legislation are those of the individual to whom the data relates. The School will however in most cases rely on parental authority or notice for the necessary ways it processes personal data relating to pupils, e.g. under the Parent Contract, or via a form. Parents and pupils should be aware that this is not necessarily the same as the School relying on strict consent.

Where consent is required, it may in some cases be necessary or appropriate, given the nature of the processing in question, and the pupil's age and understanding to seek the pupil's consent, either alongside or in place of parental consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

The School makes it clear to pupils that they should expect the School to share information about them with parents in the ordinary course of school matters (e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare. That is unless, in the School's opinion, there is a good reason to do otherwise).

However, from U3 (Year 7) and above, it will usually be for the pupil to authorise a specific subject access request made by a parent on their behalf. The School will consider other individual requests for information relating to a pupil made by a parent (and may have lawful grounds to provide it), but the School is legally obliged to consider the child's data protection rights in doing so, in particular if the information is sensitive or special category personal data.

Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds her agreement to her personal data being disclosed to her parent or parents, the School will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding her consent, or where the School believes disclosure will be in the best interests of the pupil or other pupils, or if it is under a legal obligation to disclose.

The School will only grant the pupil direct access to her own personal data if, in the School's reasonable belief, the pupil understands the nature of the request she has made, and the disclosure is made with due care for any harm or distress it may cause her.

11. Photography, Filming and Images

Photographs and moving images of identifiable individuals are personal data. The School uses them for a range of purposes, from recording a pupil's learning to promoting the School.

Lawful basis

Purpose	Lawful basis
Internal educational and pastoral use — recording learning, displays within School, EYFS learning journals, records of achievement	Legitimate interests, and contractual necessity under the Parent Contract
External publication — the public areas of the School website, social media, the prospectus, advertising, press and other marketing	Consent
Records of School events retained for archive purposes	Legitimate interests
Safeguarding, disciplinary or investigatory purposes, including CCTV	Legal obligation, and substantial public interest in respect of any special category data

Consent, granularity and withdrawal

Where the School relies on consent, that consent will be:

- specific as to purpose, so that a parent or pupil may agree to some uses and not others, e.g. internal use, the School website, social media, the prospectus and press being distinguished from one another;
- recorded, so that staff can check before an image is used; and
- capable of being withdrawn at any time, as easily as it was given, by contacting the School using the details at section 22 of this Policy.

Where consent is withdrawn, the School will cease using the image for the purposes concerned and will remove it from School-controlled channels within a reasonable period. The School will make reasonable efforts to remove images from material already published, but cannot guarantee removal from printed material already distributed, from archived press coverage, or from third-party copies or reproductions already made. The School will explain this at the point consent is sought.

Photography and image consents are recorded against each pupil's record in the School's management information system. They are collected at the point of admission and may be updated by a parent, at any time by contacting the School Office. The Data Manager is responsible for maintaining each pupil's record, and staff must check it before any image is used externally. Annual checks are made with parents to see if they still wish the withdrawal or caveat to remain. This review is carried out in September to then capture any new pupils that may not have chosen correctly at the point of entry. The processing is recorded in the School's Record of Processing Activities.

Practical rules for staff

- Photographs and video of pupils must be taken on School-provided devices and stored within School systems. Staff must not use personal devices to take or store images of pupils.

- Before publishing any image, staff must check the permission record for every identifiable pupil in it.
- No photograph on the public area of the School website will feature a pupil's full name. The School will consult those involved before using a name in connection with any image intended for external publication.
- Particular care must be taken with images showing pupils in School uniform, which may allow a pupil to be identified and located by a stranger.
- Under no circumstances may photographs or video be taken in changing rooms or lavatories.
- In the EYFS setting, parents, carers and visitors are not permitted to use personal mobile phones, cameras or other devices with imaging and sharing capability without the prior approval of the Head of Pre-Prep or the Head of Prep School.
- Images shared with parents through the School's online learning journal are visible only to School staff and to the parents of the pupil concerned.

Third parties
Where the School engages a professional photographer, a press photographer attends a School event, or a third party is permitted to film on School premises, the School will establish in writing what the images may be used for and how long they may be kept. A written agreement will be put in place where that third party is acting as the School's processor.

Parents and other guests attending School events may take photographs for their own personal and family use. The School asks that images which include other people's children are not shared on social media or forwarded beyond the immediate family.

12. Direct Marketing, Fundraising and Third-Party Promotion

The School communicates with parents, alumnae, donors and supporters about the St Catherine's Association, the Parent Teacher Association, fundraising, events, and the maintenance of relationships with former pupils.

Electronic direct marketing is regulated not only by Data Protection Legislation but also by the Privacy and Electronic Communications Regulations ("PECR"), which the Information Commissioner's Office also enforces. Where PECR applies, it applies in addition to the UK GDPR, and reliance on legitimate interests under the UK GDPR does not remove the need to comply with it.

Promotion of third-party activities
The School is frequently asked to make parents aware of activities run by external organisations, such as holiday clubs and sports camps.

The School's position is as follows:

- Sending information promoting a third party's services to parents by email, text message or other electronic means is electronic direct marketing under PECR. That remains the case even where no personal data is shared with the third party, the School receives no payment, and the communication is framed as helpful information.
- The School will therefore only send such communications to individuals who have given specific opt-in consent to receive information about third-party opportunities. That consent must be a separate, granular preference — it cannot be bundled into general consent to School communications — and it must be as easy to withdraw as it was to give.

- Passive means of making information available do not constitute electronic direct marketing and remain available to the School. These include displaying a banner on School premises, hosting information which parents choose to access, and engaging with a third party's own social media posts.
- Use of the School's name, logo or wheel device by a third party is a separate question of trademark and reputational risk, not of data protection, and remains at the School's discretion.

The School's own marketing and fundraising

The School's own fundraising, development and alumnae communications are addressed in the Alumnae, Fundraising and Association privacy notice, which sets out the lawful basis for each type of communication and how an individual may object or opt out. Every electronic marketing communication the School sends will include a means of opting out, and an opt-out will be actioned promptly.

Any individual may ask the School to limit or object to the use of their personal data for these purposes at any time, using the details at section 22.

Preferences for alumnae, development and fundraising communications are recorded against the individual's record in the School's alumnae and development database. An individual may set or change their preferences at any time by using the opt-out link in any electronic communication, or by contacting the School using the details at section 21. Preferences are applied across all electronic marketing channels.

13. Third-party Platforms, Suppliers and Processors

Where a third party processes personal data on the School's behalf it is a processor, and that engagement must be governed by a written agreement containing the provisions required by Article 28 of the UK GDPR. The School maintains a register of these agreements.

The School also carries out and documents checks on its processors' compliance, on a risk-assessed cycle. Holding a signed agreement is not by itself sufficient; the School must be satisfied on a continuing basis that the processor provides sufficient guarantees.

Staff must not engage a supplier who will handle the School's personal data or begin using a new online service or application in connection with School business, without first following the process.

New systems, applications and data protection by design

Article 25 of the UK GDPR requires the School to consider data protection when designing new processes and selecting new systems, rather than afterwards.

In practice:

- Any new cloud service, application or online platform which will hold or process personal data must be authorised by the IT Support Department before it is implemented or used. The IT Support Department carries out checks on where and how data will be held and on the supplier's data protection position.
- Where a written agreement is required, it must be in place before processing begins, and it is recorded on the processor register.
- The processing must be added to the Record of Processing Activities.

- Where the processing is likely to result in a high risk to individuals, a Data Protection Impact Assessment (DPIA) must be completed and approved by the Data Protection Officer before the processing begins. The School's DPIA Policy sets out when this is required and how it is done.

Staff must not sign up to, trial or begin using a new service which involves pupil, parent or staff personal data on their own initiative, however useful it appears. This includes free services and browser extensions, and it includes artificial intelligence tools.

Artificial Intelligence (AI)
The use of AI tools in teaching, learning and administration is addressed in the Information and Communications Technology (ICT) Policy. For data protection purposes, staff must not input pupil, parent or staff personal data into any artificial intelligence tool unless that tool has been authorised by the IT Support Department for that purpose and, where required, a Data Protection Impact Assessment has been completed.

14. International Transfers

Some of the School's processors are based outside the United Kingdom or use sub-processors who are. Transfers of personal data outside the UK are permitted where they form part of a properly authorised engagement and where an appropriate transfer mechanism is in place, that is, where the receiving country benefits from UK adequacy regulations, or where the transfer is governed by the UK International Data Transfer Agreement or by the UK Addendum to the European Commission's Standard Contractual Clauses.

The School records the transfer mechanism for each processor on its processor register and applies enhanced scrutiny where the processor handles special category data or holds personal data about a large number of individuals.

15. Disclosure of Personal Data

The School may need to share personal data it holds with third parties. Such situations include the provision of references to other educational institutions; entering pupils for public examinations; disclosure of medical information where it is in a pupil's interests; the engagement of service providers who process personal data on the School's behalf; complaints panels; reporting incidents or providing safeguarding data to the relevant authorities in accordance with the School's duties under law and statutory guidance, including Keeping Children Safe in Education; and responding to requests from government departments, public authorities and regulatory bodies.

The full description of who the School shares personal data with, and why, is given in its Privacy Notices and in its Record of Processing Activities.

Where the School receives a disclosure request from a third party, it will take reasonable steps to verify the identity of that third party before making any disclosure. Staff who receive an unexpected request for personal data from any external party must refer it to the Data Protection Officer rather than responding to it.

16. Exemptions

In some circumstances Data Protection Legislation provides exemptions from particular provisions of the UK GDPR and from individual rights. This means, for example, that the School may be required or permitted to

process or share personal data for certain specific purposes without reference to the individuals concerned, including:

- for the prevention or detection of crime;
- in certain scenarios when engaging with local authorities;
- for the assessment of any tax or duty; and
- where required by law or in connection with legal proceedings, or subject to a request from a competent statutory authority.

These are examples only. Further information about the exemptions is published by the Information Commissioner's Office. Whether an exemption applies in a given case is a decision for the Data Protection Officer.

17. Accuracy and Completeness

The School will endeavour to ensure that all personal data held in relation to an individual is accurate.

Individuals must notify the School of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected, although the School may reasonably determine whether or not the information is in fact accurate.

18. Retention of Personal Data

The School will retain personal data securely and only for as long as is necessary for a legitimate and lawful reason. Retention periods differ considerably between types of record: some are set by statute, and safeguarding and incident records are kept for substantially longer than ordinary records.

The periods that apply to each category of record are set out in the School's Information and Records Retention Policy and Retention Schedule. Staff responsible for managing the destruction of personal data must work to that schedule.

A limited and reasonable amount of information will be kept for archiving purposes. Where an individual has asked the School not to keep in touch with them, the School will need to retain a record of that fact in order to give effect to their wishes; this is known as a suppression record.

The School will often have lawful and necessary reasons to retain some personal data even following a request for its erasure.

19. Data Security

The School must ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data, and against its accidental loss, destruction or damage.

The School takes appropriate steps to ensure that members of staff have access only to the personal data necessary for their role, and only where they are suitably trained and competent. Access to the School's management information system and its other core systems is granted on a role basis and reviewed regularly.

The technical measures the School applies, and the rules governing devices, accounts, passwords, remote access, removable media, the handling of paper records and secure disposal, are set out in the Information

Security Policy and in the Information and Communications Technology (ICT) Policy. All staff are required to comply with both.

20. Training

All staff, governors, contractors, agency staff, peripatetic staff, volunteers, work experience students and gap year placement students will be made aware of this Policy and of their duties under Data Protection Legislation.

All staff receive data protection and cyber security training on induction and refresher training thereafter. Training is delivered through the School's online training platform, supplemented by briefings where a specific risk or change in the law requires it. Governors and regular volunteers receive training appropriate to their role. Records of attendance, content and date are maintained by the HR department.

21. Complaints, Contact and Enforcement

Any individual wishing to exercise their data protection rights, including access, rectification, erasure, restriction, or transfer of their personal data, or to raise a concern regarding the handling of their personal data, may do so in writing:

By email: GDPR@stcatherines.info
By post: Caroline Mead, Data Protection Officer, St Catherine's School, Station Road, Bramley, Guildford, Surrey, GU5 0DF
Telephone: 01483 893363

Complaints relating to the handling of personal data will be managed in accordance with the UK GDPR and section 164A of the Data Protection Act 2018. The School will acknowledge such complaints within 30 days of receipt in writing, investigate them while keeping the complainant updated on progress and without undue delay, and provide a clear outcome. Where appropriate, complaints will be managed alongside the School's Complaints Policy and procedures to ensure compliance with both the Independent School Standards and data protection legislation.

If an individual is not satisfied with the School's response, or if the School has failed to respond within the appropriate timeframe, they have the right to escalate their complaint to the ICO:

Information Commissioner's Office
Website: ico.org.uk
Telephone: 0303 123 1113

The School and the Information Commissioner's Office both recommend that an individual raises the matter with the School first.

22. Related Policies and Documents

This Policy should be read in conjunction with:

Document	Relationship to this Policy
Privacy Notice - Pupils and Parents	Tells pupils and parents what the School does with their personal data
Privacy Notice - Staff, Governors, Volunteers and Contractors	As above, for those working at or for the School
Privacy Notice - Applicants (Pupil Admissions)	As above, for prospective pupils and their parents
Privacy Notice - Applicants (Staff Recruitment)	As above, for job applicants
Privacy Notice - Alumnae, Fundraising and the St Catherine's Association	As above, including the School's marketing position
Privacy Notice - Website Visitors and Cookies	As above, for visitors to the School's website
Appropriate Policy Document	The Schedule 1 conditions and safeguards for special category and criminal offence data
Information and Records Retention Policy, and Retention Schedule	How long each type of record is kept
Information Security Policy	Organisational and physical security measures
Information and Communications Technology (ICT) Policy	Technical security measures, acceptable use, online safety and conduct
Data Breach Policy	How personal data breaches are reported, assessed and recorded
Subject Access Request Procedure	How subject access and other rights requests are handled
Data Protection Impact Assessment (DPIA) Policy	When a DPIA is required and how it is carried out
CCTV Policy	The School's use of closed circuit television
Safeguarding and Child Protection Policy	Including pastoral confidentiality and what staff may promise a pupil
Complaints Policy	The School's general complaints procedure
Record of Processing Activities	The School's record of what personal data it processes and why