The Cornwall Independent School

GDPR DATA PROTECTION POLICY

Incorporating the UK GDPR, the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025), and the Data Protection Complaints Procedure required from 19 June 2026, as substantially amended by the Data (Use and Access) Act 2025 (DUAA 2025). The policy has accordingly been renamed "Data Protection Policy", which is also the naming convention used in Independent School Standards (ISS) Guidance, DfE model documentation and ICO resources for schools.

This document, which applies to the whole school, including the Early Years Foundation Stage (EYFS – Reception Class) and Key Stages 1 to 4 inclusive, is available on request from the School Office, and can be made available in large print or another accessible format if required.

We have a whole-school approach to safeguarding, which is the golden thread that runs throughout every aspect of the school. All our school policies support our approach to safeguarding (child protection). Our fundamental priority is our children and their wellbeing; this is first and foremost.

Scope: This policy is a live document that is sensitive to our working practices and is subject to change according to the needs of The Cornwall Independent School (TCIS). All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures, both within and outside of normal school hours, including activities away from school. All employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the *Policies Register*.

Legal Status: This policy meets the requirements of the Education (Independent School Standards) Regulations 2014 (as amended), the Independent School Standards: Guidance for independent schools (DfE, April 2026), Keeping Children Safe in Education (KCSIE), the EYFS Statutory Framework for group and school-based providers, and other statutory and best practice documentation cited in this document.

Monitoring, Review and Adaptation: The text of this policy **is necessary** and proportionate to meet the needs of The Cornwall Independent School, supporting those who work with our pupils and **making clearer** the responsibilities of school staff, volunteers, the Proprietor and the Governance Advisory Body. These arrangements are subject to continuous monitoring, refinement, and audit by the Headteacher. The Governance Advisory Body is committed to regularly reviewing and updating our policies to ensure they remain relevant and effective, including the efficiency with which related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated or reviewed arrangements, in writing or electronically.

The Policy Owner is Mrs Rebecca Stevens, supported by the Education and Compliance Officer.

Reviewed: September 2026
Next Review: September 2027 (or sooner, to reflect any material change in statutory or best practice requirements)

Miss Louise Adams
Headteacher

Contents:

Related documents:

- Safeguarding (Child Protection) Policy, including Confidentiality and Information Sharing
- Online Safety Policy and Acceptable Use of ICT Agreements
- Mobile Phones and Devices Policy
- Photography, Filming and Use of Images Policy
- Complaints Policy (incorporating the Data Protection Complaints Procedure from 19 June 2026)
- CCTV and Biometric Data Privacy Notice
- Records Retention Schedule
- Privacy notices for pupils, parents, staff, job applicants and visitors
- EYFS-specific policies (Missing pupils, Use of Mobile Devices/Cameras, Non-Collection of Children)

Aims: The Cornwall Independent School (TCIS) is committed to ensuring that all personal data related to pupils, staff, parents/carers, governors, volunteers, visitors and other individuals is collected, stored and disposed of fairly, lawfully, transparently and securely, in accordance with the UK General Data Protection Regulation (UK GDPR) the Data Protection Act 2018 (DPA 2018) as amended by the Data (Use and Access) Act 2025 (DUAA 2025). This policy applies to all personal data processed by or on behalf of the school, regardless of whether it is held in paper or electronic format, and to every member of the school community, including pupils in the Early Years Foundation Stage (EYFS – Reception) and across Key Stages 1 to 4.

Legislation and guidance: This policy meets the requirements of the GDPR and the DPA 2018, as amended by the DUAA 2025. It is based on guidance published by the Information Commissioner's Office (ICO), including the ICO's guide to subject access and its guidance on data protection complaints.

Governance reform note: the DUAA 2025 reforms the ICO from a "corporation sole" (a single Information Commissioner) into a body corporate, the Information Commission, governed by a board. At the date of this policy the transition date has not been confirmed and the regulator continues to operate and be publicly known as the ICO. This policy therefore uses "ICO" as the current operative term and will be updated to "Information Commission" once the transition formally takes effect; no substantive duty in this policy changes as a result of the rename.

It meets the requirements of the Protection of Freedoms Act 2012 in relation to biometric data (see section 19)

It also reflects the surveillance camera code of practice issued under the Protection of Freedoms Act 2012, and ICO guidance on video surveillance (see Section 20.)

It complies with the Education (Independent School Standards) Regulations 2014, as amended, and the Independent School Standards: Guidance for independent schools (DfE, April 2026) ("ISS Guidance 2026"), in particular Standard 33 and paragraphs 7.3–7.5 on data protection complaints.

It has regard to Keeping Children Safe in Education (KCSIE) 2026, including the treatment of cybersecurity as a safeguarding matter, the requirement for an annual filtering and monitoring review, and updated information-sharing expectations on pupil transfer.

It has regard to the EYFS Statutory Framework for group and school-based providers (effective 1 September 2025), including paragraph 3.6 on the use of mobile phones, cameras and any other device capable of capturing or sharing images in the EYFS setting.

It reflects the information-sharing duty and the provision for a Single Unique Identifier for children inserted into the Children Act 2004 (new sections 16LA–16LC) by the Children's Wellbeing and Schools Act 2026 (CWSA 2026) (see Section 11).

It notes that the CWSA 2026 also inserts a regulation-making power into Article 8 of the UK GDPR, enabling the Secretary of State to change the age of digital consent, or how a child's age is verified for online services. No such regulations have been made at the date of this policy; the DPO will monitor developments and this policy, and the age referred to in Section 9, will be updated without delay if regulations are made.

It has regard to the ICO's Children's code (Age-Appropriate Design Code) where the school provides, or procures from a third party, online services that are aimed at, or likely to be accessed by, pupils.

It complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 insofar as that regulation is capable of applying; however, as TCIS is an independent school and not a local-authority-maintained school, the 15-school-day statutory right of access in those Regulations does not bind TCIS directly (see Section 14 for TCIS's approach).

Freedom of Information note: TCIS is an independent school and is not a "public authority" for the purposes of the Freedom of Information Act 2000. TCIS does not operate a publication scheme under that Act. Requests for information about the school are handled under this policy (where the request concerns personal data) or under the Complaints Policy.

Definitions:

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individuals: 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 category data	Personal data, which is more sensitive and so needs more protection, including information about an individual: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, 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. TCIS, acting through its Proprietor, is the data controller.

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 (e.g. a cloud software supplier).
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Recognised legitimate interest	A legitimate interest that Parliament has pre-approved under Article 6(1)(ea) UK GDPR (inserted by the DUAA 2025), for which the usual legitimate interests balancing test is not required — for example, safeguarding a child from harm or neglect, crime prevention and detection, and responding to an emergency (see Section 8).
Automated decision-making (ADM)	A decision made about an individual using only automated means (which may include artificial intelligence), without meaningful human involvement, that produces a legal effect or similarly significant effect on that individual (see Section 12).

The data controller: The Cornwall Independent School processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller. The Cornwall Independent School, through its proprietor, is registered as a data controller with the ICO and will renew this registration annually, or as otherwise legally required. TCIS maintains a record of its processing activities (ROPA) as required by the accountability principle (see Section 6).

Roles and responsibilities:

- Proprietor
  - The Proprietor has delegated specific duties and responsibilities to the Governance Advisory Board. The proprietor is responsible for ensuring that The Cornwall Independent School complies with all relevant data protection obligations.

- Data Protection Officer
  - The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, handling data protection complaints under Section 15, and developing related policies and guidance. At The Cornwall Independent School, the DPO is Mrs Tracey Rowe (Bursar)

- Reporting to the Governance Advisory Board
  - The DPO will provide an annual report of their activities to the Governance Advisory Board in the summer term and, where relevant, will report on data protection issues, complaints and breaches during the year. The DPO is the first point of contact for individuals whose data the school processes, and for the ICO.

- The Designated Safeguarding Lead (DSL) and cybersecurity
  - Because KCSIE 2026 frames cybersecurity as a safeguarding matter, the DPO and the DSL will work closely together, in particular on the annual filtering and monitoring review, cyber-incident response, and information sharing on pupil transfer. The DSL retains overall responsibility for filtering and monitoring and must be able to articulate what the school's systems do; the DPO advises on the data protection implications.

- 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;
- reporting to the DPO, within 24 hours of becoming aware, any suspected data protection complaint (Section 15) or personal data breach (Section 25), 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, or deal with data protection rights invoked by an individual;
- if there has been a data breach – refer to The Cornwall Independent School Data Breach Procedure;
- whenever they are engaging in a new activity that may affect the privacy rights of individuals and if they need help with any contracts or sharing personal data with third parties, including any new AI or EdTech tool (see Section 12).

Data protection principles: The UK GDPR is based on data protection principles with which The Cornwall Independent School must comply. 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; and
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

TCIS must also be able to demonstrate compliance with the above (the accountability principle). This policy, together with the school's ROPA, privacy notices, data protection impact assessments (DPIAs) and training records, is the school's primary evidence of accountability.

Lawful bases for processing personal data: The Cornwall Independent School will only process personal data where it has one of six lawful bases to do so:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can comply with a legal obligation.
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, carrying out a task in the public interest or exercising official authority, can perform its official functions.
- The data needs to be processed for the legitimate interests of the school or a third party, including a recognised legitimate interest (see Section 8), 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 category data, TCIS will also meet one of the special category conditions for processing which are set out in Article 9 UK GDPR and Schedule 1 to the Data Protection Act 2018 (for example, the substantial public interest condition, which frequently applies to safeguarding processing).

Recognised legitimate interests: The DUAA 2025 inserted a new Article 6(1)(ea) into the UK GDPR, creating a list of "recognised legitimate interests" for which the usual legitimate interests balancing test does not need to be carried out. The categories most relevant to TCIS are:

- disclosing personal data to a body with statutory crime-prevention or safeguarding functions (for example, the police or children's social care) to prevent, detect or investigate crime, or to protect a child or vulnerable adult from harm or neglect;
- processing necessary to respond to an emergency, including a threat to the life, health or safety of a person;

- disclosures reasonably necessary for another organisation to perform a public task set out in law (for example, providing information to Ofsted, the Independent Schools Inspectorate (ISI) or the Department for Education).

A recognised legitimate interest removes the need for a full balancing test in respect of Article 6 only. Where the information concerned is special category data (for example, safeguarding, health or welfare information), a separate Article 9 condition — most commonly the substantial public interest condition at Schedule 1 DPA 2018 — must still be identified before the information is shared. All disclosures made in reliance on a recognised legitimate interest are recorded in the school's safeguarding or data-sharing log, with the specific category relied upon noted.

Children, consent and special category data: If TCIS offers online services to pupils, such as classroom or subject apps which require the use of personal data and intends to rely on consent as the lawful basis, the school will obtain parental consent for pupils who are under the digital age of consent, currently 13 under Article 8 UK GDPR. As set out in Section 2, the Secretary of State has a (not yet exercised) power under the CWSA 2026 to change this age or the way a child's age is verified; TCIS will update this policy without delay if that power is used.
Whenever TCIS first collects personal data directly from individuals, it will provide the relevant privacy information required by data protection law. Where TCIS procures or recommends an online service or app that is aimed at, or likely to be accessed by, pupils, the DPO will have regard to the ICO's Children's code (Age-Appropriate Design Code) in assessing the product before it is adopted.

Limitation, minimisation and accuracy: TCIS will only collect personal data for specified, explicit and legitimate reasons, which will be explained to individuals when their data is first collected. If personal data is to be used for a new reason, individuals will be informed before this happens and consent sought where necessary. Staff must only process personal data where it is necessary to do their jobs and must ensure data is deleted or anonymised once it is no longer needed.

Sharing personal data: We will not normally share personal data with anyone else, but may do so where:

- 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, save where a recognised legitimate interest or the safeguarding information-sharing duty described below applies;
- our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies – the school will only appoint suppliers who can provide sufficient guarantees of compliance with data protection law, will put a data sharing or processing agreement in place, and will only share the data the supplier needs.
- the disclosure is made under a recognised legitimate interest (Section 8), for example to the police for crime prevention, or in an emergency;
- the disclosure is required to satisfy the school's safeguarding obligations, including under the information-sharing duty for the purposes of safeguarding and promoting the welfare of children inserted into the Children Act 2004 (new sections 16LA–16LC) by the CWSA 2026;
- the disclosure is 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, or in connection with legal proceedings;
- the disclosure is for research and statistical purposes, provided personal data is sufficiently anonymised or consent has been given.

Single Unique Identifier: the CWSA 2026 allows the Secretary of State to designate, by regulations, a consistent identifier ("Single Unique Identifier") for children and to specify which agencies ("designated persons") must record and use it when processing information for safeguarding purposes, supported by a Code of Practice. No regulations designating independent schools as designated persons had been made at the date of this policy. The DPO maintains a watching brief and will update the school's safeguarding information-sharing procedures if and when TCIS becomes a designated person.

TCIS 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 outside the UK we will do so in accordance with Section 22.

Automated decision-making and profiling (including AI): The DUAA 2025 reformed Article 22 UK GDPR. Solely automated decision-making, including decisions informed by artificial intelligence (for example AI-assisted marking, plagiarism/AI-use detection tools, adaptive learning or assessment platforms, or automated screening in admissions), is now permitted more broadly than before, provided appropriate safeguards are in place.

Where TCIS uses, or considers using, a tool that makes solely automated decisions with a legal or similarly significant effect on a pupil, parent or member of staff, the school will:

- carry out a data protection impact assessment (DPIA) before the tool is adopted;
- tell individuals that a decision is, or may be, automated;
- give individuals the right to request meaningful human review of the decision, and to express their point of view and contest the outcome;
- not rely solely on automated or AI-generated output for a decision that has a significant effect on a pupil or member of staff — for example exclusion, a safeguarding referral, or an examination outcome — without meaningful human review.

This section is cross-referenced with the generative AI provisions of KCSIE 2026 and with the school's Online Safety Policy, which addresses the acceptable use of AI tools by staff and pupils.

Subject access requests and other rights of individuals: Individuals have a right to make a 'subject access request' to gain access to personal information that The Cornwall Independent 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 must be submitted in writing, either by letter or email to the DPO. They should include:

- name of individual;
- correspondence address;
- contact number and email address and
- details of the information requested.

If staff receive a subject access request, they must immediately forward it to the DPO.
Personal data about a child belongs to that child. However, we would expect parents to exercise this right on behalf of a child who does not have sufficient understanding to make the request themselves (see Section 14)

Timescales, clarification and "stopping the clock":
Following the changes made by the DUAA 2025, when responding to requests TCIS will:

- may ask the individual to provide up to two forms of identification, and may contact the individual to confirm the request was made;
- respond without undue delay and, at the latest, within one month of the "relevant time period" beginning — that is, from whichever is the later of receipt of the request, receipt of any information reasonably needed to confirm identity or authority, and payment of any fee;
- where a request is broad or unclear, may ask the individual for reasonable clarification of the information sought; this "stops the clock" on the response deadline from the day clarification is requested until the day after a response is received. An individual cannot be required to narrow their request, and if they simply repeat the original request, the school will carry out a full search;
- may extend the response period by up to a further two months (three months in total) where a request is complex or numerous, informing the individual within the first month and explaining why the extension is necessary;
- will provide the information free of charge, save where a request is manifestly unfounded or excessive (for example, because it is repetitive), in which case the school may charge a reasonable fee reflecting administrative cost, or refuse to act on it, giving reasons and informing the individual of their right to complain (see Sections 15 and 16);

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual;

- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- is contained in adoption or parental order records;
- is given to a court in proceedings concerning the child.

Parental and pupil access to see the educational record:
The Education (Pupil Information) (England) Regulations 2005, which give parents at local-authority-maintained schools a 15-school-day right of access to their child's educational record, do not apply to independent schools. This policy has been corrected accordingly;

TCIS's approach is set out below*:*
As TCIS is an independent school, a request from a parent, or a person with parental responsibility, to see a child's educational record is treated as a subject access request under the UK GDPR and DPA 2018 (see Section 13), and not as a request under the 2005 Regulations. As a matter of good practice and transparency, TCIS aims, wherever reasonably possible, to provide the educational record within 15 school days of a clear written request; the statutory maximum response time, however, remains one month, extendable as described in Section 13.
Where a pupil has sufficient age and understanding to exercise their own data protection rights (sometimes referred to as "Gillick competence"), the request and the underlying data belong to the pupil, and TCIS will engage directly with the pupil as appropriate to their age and maturity. For younger pupils, TCIS will normally expect a parent or person with parental responsibility to make and receive the request on the child's behalf, acting in the child's best interests.

Data protection complaints procedure:
From 19 June 2026, section 103 of the DUAA 2025 inserts a new section 164A into the DPA 2018, giving anyone who believes TCIS has infringed data protection legislation in the way it has handled their personal information the right to complain to the school directly, before referring the matter to the ICO. TCIS is the first point of contact for such complaints, not the ICO.
In line with ICO guidance (cited at ISS Guidance 2026, paragraph 7.3) and ISS Guidance 2026 paragraphs 7.3–7.5 (Standard 33), TCIS has not created a wholly separate, standalone complaints process but has adapted its existing Complaints Policy and this policy to meet the new statutory obligations. A summary of the procedure is set out below; the full procedure is at Appendix 2.

- How to complain: a data protection complaint should be made in writing (letter, email or online form) to the DPO, Mrs Tracey Rowe, or via the school's general Complaints Policy, which has been adapted to route data protection complaints to the DPO.
- Acknowledgement: TCIS will acknowledge receipt of a data protection complaint within 5 school days.
- Investigation: the DPO will investigate the complaint, keeping the complainant informed of progress, and will respond substantively without undue delay — TCIS's target is within 20 school days of acknowledgement, extended where the matter is complex, with reasons given to the complainant.
- Record-keeping: every data protection complaint is logged by the DPO, distinct from (but cross-referenced with) general school complaints, subject access requests and safeguarding disclosures, so that the school can demonstrate compliance with section 164A.
- Escalation: if the complainant remains dissatisfied with TCIS's response, they may refer the complaint to the ICO (ico.org.uk or 0303 123 1113). The ICO will not normally investigate a complaint unless the school has first had the opportunity to resolve it.

Reception staff, the DPO and members of the Senior Leadership Team are briefed on the new statutory route, so that a data protection concern raised informally at first contact (for example, at the school office or by telephone) is correctly identified and routed to the DPO rather than being treated only as a general enquiry.

Other data protection rights of the individual: In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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 or legitimate interests, including a recognised legitimate interest;
- request a copy of agreements under which their personal data is transferred internationally (see Section 22);
- object to decisions based solely on automated decision making or profiling, and request meaningful human review (see Section 12);
- prevent processing that is likely to cause damage or distress;
- be notified of a data breach in certain circumstances (see Section 25);
- make a complaint, first to TCIS (see Section 15) and, if unresolved, to the ICO;
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).
- Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Disclosure of information to third parties:
The Cornwall Independent School may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. The Cornwall Independent School confirms that it will not generally disclose information unless the individual has given consent, a recognised legitimate interest applies, or one of the specific exemptions under data protection law applies. However, The Cornwall Independent School does intend to disclose such data as is necessary to third parties for the following reasons:

- to give a confidential reference.
- to give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend.
- to publish results of public examinations or other achievements.
- to disclose details of a pupil's medical condition where it is in the pupil's interest to do so, e.g. organisers of school trips.

Where The Cornwall Independent 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.

Photographs and videos and images: As part of school activities, we may take photographs and record images of individuals within The Cornwall Independent School.
We will obtain written consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent/carer. Uses may include:

- within The Cornwall Independent School on notice boards, school posters, prospectus and newsletters, etc.;
- outside of school by external agencies such as the school photographer, newspapers, campaigns;
- online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, beyond the first name, where necessary to ensure they cannot be identified.
This section is read alongside the EYFS Statutory Framework, paragraph 3.6, which extends beyond phones and cameras to any device capable of capturing or sharing images — including tablets, smart watches and other wearables — and the school's Mobile Phones and Devices Policy. TCIS also has regard to KCSIE 2026's treatment of AI-generated or "deepfake" images and self-generated intimate images as forms of child-on-child abuse where images are misused; any such incident is treated as a safeguarding matter in the first instance and reported under the Safeguarding (Child Protection) Policy, in addition to any data protection considerations.

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 DPO, 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 section 6;)

- completing privacy impact assessments where The Cornwall Independent School processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Regularly 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, making available the name and contact details of The Cornwall Independent School and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - for all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Biometric Data:

Where TCIS uses a pupil's biometric data (for example, fingerprint recognition for cashless catering or library systems), it will comply with the Protection of Freedoms Act 2012:

- written consent will be obtained from at least one parent or person with parental responsibility before a pupil's biometric data is first processed, and TCIS will act on a written objection from any parent, even where another parent has given consent;
- a pupil may separately object, or refuse to participate, even if their parent(s) have given consent, and TCIS will not process that pupil's biometric data if they object;
- TCIS will provide a reasonably practicable alternative means of access to the service (for example, a PIN or card) for any pupil whose biometric data is not, or can no longer be, processed;
- consent may be withdrawn at any time, and a register of consents, objections and withdrawals is kept by the DPO.

CCTV and other surveillance:

Where TCIS operates CCTV or other surveillance systems, for example for site security and safeguarding at entrances and around the school perimeter, this is done in accordance with the surveillance camera code of practice issued under the Protection of Freedoms Act 2012 and ICO guidance on video surveillance. Signage is displayed to notify individuals that CCTV is in operation, access to footage is restricted to authorised staff, and footage is retained only for as long as necessary before being securely deleted, unless required for an ongoing investigation. A CCTV privacy notice is available on request from the School Office. CCTV is not used in areas where individuals have a reasonable expectation of privacy, such as toilets or changing rooms, other than in exceptional and proportionate circumstances agreed in advance by the Headteacher and the DPO on safeguarding grounds.

Data Protection by design and default:

TCIS will put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- appointing a suitably qualified DPO and ensuring they have the resources needed to fulfil their duties and maintain their expert knowledge;
- only processing personal data that is necessary for each specific purpose, in line with the data protection principles (Section 6);
- completing data protection impact assessments (DPIAs) where processing presents a high risk to individuals' rights and freedoms, including before introducing new technologies, AI tools or EdTech platforms (the DPO will advise on this process and will have regard to the ICO's Children's code where a product is aimed at, or likely to be accessed by, pupils);
- integrating data protection into internal documents, including this policy, related policies and privacy notices;
- regularly training staff on data protection law, this policy and related matters, and keeping a record of attendance (see Section 26);
- regularly conducting reviews and audits to test privacy measures and confirm compliance;
- maintaining a record of processing activities (ROPA), including the categories of data, purposes of processing, third-party recipients, retention periods and security measures for each significant processing activity.

International transfers:

Where a supplier or cloud service provider processes personal data outside the United Kingdom, TCIS will ensure the transfer is protected by UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, or another lawful transfer mechanism recognised by the ICO, and that the DPO has completed appropriate due diligence on the recipient before the transfer takes place. A list of TCIS's key overseas processors and the safeguards in place is maintained by the DPO as part of the ROPA.

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 or are encrypted and password protected;
- 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 it must be safeguarded, papers should be carried in locked bags or cases. The use by staff of removable media e.g. USB sticks is not permitted, unless password protected;
- strong, unique passwords (and multi-factor authentication, where available) are used to access school computers, laptops and other electronic devices;
- staff, pupils 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 *Online safety policy* and *Acceptable use agreements*);
- 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 (see section 11).

This section is cross-referenced with the DfE's Digital and Technology Standards (filtering and monitoring, last updated March 2025) and KCSIE 2026, under which the school carries out a documented annual filtering and monitoring review with a named review team, an annual cyber risk assessment, and annual cybersecurity training for all staff and at least one governor, applying filtering and monitoring to staff accounts as well as pupil accounts.

Data held electronically: Personal data is held on the TCIS network within secure databases. All confidential data held on staff, pupils and parents is restricted to key individuals and requires a username and password for access. Access to network folders is further restricted by the Network and IT Support arrangements. Files containing confidential personal information are password protected. Data on individuals that TCIS would like to feature on the school website will not be posted without appropriate permission. Access to confidential data is restricted to a minimum number of people.

Hard copy data: Hard-copy personal data about pupils is kept in lockable filing cabinets by authorised users. Staff personal data is stored in personnel files held in the COO and HR office. Personal data about parents held by the school is kept securely by the COO. Access to confidential data is limited to the minimum number of people necessary.

Retention and 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 Cornwall Independent School behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. Specific retention periods for different categories of record are set out in TCIS's Records Retention Schedule, which the DPO maintains with reference to sector guidance such as the IRMS Records Management Toolkit for Schools. The DUAA 2025 also gives organisations greater flexibility to repurpose existing datasets for research, statistical or archiving purposes without needing fresh consent, provided appropriate safeguards are applied; TCIS anticipates this will rarely be relevant, but the DPO will apply it, for example, only to sufficiently anonymised historic attainment data used for internal quality assurance.

Personal data breaches: The Cornwall Independent 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 *Data Breach Procedure* attached to this Policy. When appropriate, we will report the data breach to the ICO within 72 hours. As example, breaches in a school context may include, but are not limited to: a non-anonymised dataset being published on the school website; safeguarding

information being made available to an unauthorised person; the theft of a school laptop containing personal data about pupils.

Training: All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, including annual cybersecurity training for all staff and at least one governor, in line with the DfE's Digital and Technology Standards and KCSIE 2026. The DPO undertakes regular CPD to maintain the expert knowledge required to fulfil their role.

Monitoring arrangements: The DPO is responsible for monitoring and reviewing this policy, which will be reviewed at least annually by the DPO and the Governance Advisory Board, or sooner where there is a material change in the law, ICO guidance, or following a significant data protection complaint or personal data breach.

Links with other policies: This data protection policy is linked to our:

- Safeguarding (Child Protection) Policy and procedures.
- Safeguarding – Confidentiality and Information Sharing
- Online Safety Policy and Acceptable use of ICT Agreements
- Photography, Filming and Use of Images Policy
- Complaints Policy (incorporating the Data Protection Complaints Procedure from 19 June 2026)
- CCTV and Biometric Data Privacy Notice
- Records Retention Schedule
- Privacy notices for pupils, parents, staff, job applicants and visitors
- EYFS-specific policies (Missing Pupils, Use of Mobile Devices/Cameras, Non-Collection of Children)

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
2. The DPO will investigate the report and determine whether a breach has occurred, considering whether personal data has been accidentally or unlawfully lost, stolen, destroyed, altered, disclosed or made available where it should not have been, or made available to unauthorised people.
3. The DPO will alert the Headteacher and the Chair of the Governance Advisory Board.
4. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff or data processors where necessary (see specific actions below).
5. The DPO will assess the potential consequences, based on how serious they are and how likely they are to occur.
6. The DPO will decide, on a case-by-case basis, whether the breach must be reported to the ICO, considering whether it is likely to negatively affect people's rights and freedoms and cause physical, material or non-material damage, including loss of control over their data, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality, or any other significant economic or social disadvantage.
7. If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
8. The DPO will document the decision, either way, in case it is later challenged by the ICO or an affected individual. Documented decisions are stored on the school's secure admin network, accessible to the admin team and leadership team.
9. Where the ICO must be notified, the DPO will do so via the ICO's 'report a breach' service within 72 hours, setting out (as far as possible): a description of the nature of the breach, including the categories and approximate number of individuals and records concerned; the name and contact details of the DPO; a description of the likely consequences; and a description of the measures taken or proposed to address the breach and mitigate its effects. If not all details are known within 72 hours, the DPO will report what is known, explain the delay and the reasons for it, and submit the remaining information as soon as possible.
10. The DPO will assess the risk to individuals and, if the risk is high, will promptly inform, in writing, all individuals whose personal data has been breached, setting out the DPO's contact details, the likely consequences, and the measures taken or proposed to mitigate any adverse effects.
11. The DPO will notify any relevant third parties who can help mitigate the loss to individuals, for example the police, insurers, banks or credit card companies.
12. The DPO will document each breach, whether or not it is reported to the ICO, recording the facts and cause, the effects, and the action taken to contain it and prevent recurrence (such as more robust processes or further staff training). Records of all breaches are stored on the school's secure admin network. The DPO and Headteacher will meet, as soon as reasonably possible, to review what happened and how recurrence can be prevented.

Actions to minimise the impact of specific types of data breach

TCIS will take the actions set out below to mitigate the impact of different types of data breach and will review the effectiveness of these actions and amend them as necessary after any breach.

Sensitive information disclosed via email (including safeguarding records):

- the sender must attempt to recall the email as soon as they become aware of the error;
- staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware;
- if the sender is unavailable or cannot recall the email, the DPO will ask the IT provider to attempt to recall it;
- where recall is unsuccessful, the DPO will contact the unauthorised recipients, explain the error, and request that they delete the information and do not share, publish, save or replicate it, obtaining written confirmation of compliance;
- the DPO will check whether the information has been made public and, if so, will contact the publisher or website administrator to request removal.

Non-anonymised pupil exam results or staff pay information shared with governors:

- paper documents are recalled and shredded; where sent by email, governors must only access it using encrypted email and will be asked to delete it, confirming in writing that they have done so.

A device containing unencrypted sensitive personal data is stolen or hacked:

- the incident is reported to the police as soon as possible;
- if a school-registered device, the DPO contacts the IT supplier to wipe the device remotely as soon as possible;
- if a personal device, the staff member must use their cloud provider to wipe the device and confirm this in writing;
- the DPO assesses what details could be accessible and will report to parents and, if appropriate, to the ICO.

The school's cashless payment provider is hacked and parents' financial details are stolen:

- the school will immediately seek details of the breach from the provider;
- parents will be notified immediately and advised to change their passwords if they consider they may be at risk.

Appendix 2: Data protection complaints procedure (section 164A DPA 2018)

This procedure implements section 164A of the DPA 2018, inserted by section 103 of the DUAA 2025, effective 19 June 2026, and ISS Guidance 2026 paragraphs 7.3–7.5 (Standard 33). It is a section of the school's Complaints Policy, adapted to meet this specific statutory obligation rather than a wholly new, standalone process.

Stage	Action
Receipt	Complaint received in writing (letter, email or online form) by the DPO, reception, or any member of staff, who forwards it to the DPO immediately.
Triage	DPO confirms the complaint concerns the handling of personal data (as distinct from a general school complaint, a subject access request, or a safeguarding disclosure) and logs it in the data protection complaints register.
Acknowledgement	DPO writes to the complainant confirming receipt, explaining the process and timescale, and asking any clarifying questions.
Investigation	DPO investigates, involving the Headteacher, DSL and/or relevant staff as needed, and keeps the complainant updated on progress.
Response	DPO provides a substantive written response, explaining the outcome, any remedial action taken, and the complainant's right to escalate to the ICO if dissatisfied.
Record and review	DPO records the complaint, outcome and any lessons learned in the data protection complaints register and reports a summary to the Governance Advisory Board.
Escalation	If dissatisfied, the complainant may refer the matter to the ICO (ico.org.uk / 0303 123 1113).

Complaints that clearly relate to safeguarding (for example, a concern about how a child protection disclosure was made) are handled in the first instance under the Safeguarding (Child Protection) Policy, with the DPO consulted on any data protection dimension. Complaints that are, in substance, a request for information (a subject access request) are redirected to the process at Section 13 of this policy, without prejudice to the complainant's right also to raise a data protection complaint about how that request was handled.

Appendix 3: Summary of key legislative and regulatory changes for September 2026

This appendix summarises, for governors' and auditors' reference, the principal legislative and regulatory changes reflected in this revised policy.

Change	Effective
Data (Use and Access) Act 2025 (DUAA 2025) — general amendments to UK GDPR/DPA 2018	Rolling, largely in force by Feb 2026
DUAA 2025 s.103 — new s.164A DPA 2018: internal data protection complaints route	19 June 2026
DUAA 2025 — "recognised legitimate interests" (Art 6(1)(ea) UK GDPR)	In force
DUAA 2025 — reformed automated decision-making (Art 22 UK GDPR)	In force
DUAA 2025 — SAR "stop the clock", reasonable and proportionate search	In force
DUAA 2025 — ICO reconstituted as the Information Commission	Date to be confirmed
Children's Wellbeing and Schools Act 2026 (CWSA 2026) — information-sharing duty and Single Unique Identifier (Children Act 2004, ss.16LA–16LC)	Royal Assent 29 April 2026; phased
CWSA 2026 — regulation-making power to change UK GDPR Art 8 digital age of consent	Power created; regulations not yet made
Independent School Standards Guidance (April 2026), Standard 33, paragraphs 7.3–7.5	April 2026
KCSIE 2026 — cybersecurity as safeguarding; annual filtering and monitoring review	1 September 2026
EYFS Statutory Framework — devices/imaging (paragraph 3.6)	1 September 2025
Correction: Education (Pupil Information) (England) Regulations 2005 do not apply to independent schools	N/A — correction of prior error
Correction: Freedom of Information Act 2000 does not apply to TCIS	N/A — correction of prior error
Policy renamed from "GDPR Data Protection Policy" to "Data Protection Policy"	This revision