



Privacy Notice for our Pupils (how we use pupil information)

About us

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This notice explains how we collect, store and use personal data about pupils at our school, like you.

We, at SMART, are a data controller for the purposes of the General Data Protection Regulation (GDPR). This means that we are responsible for deciding how we hold and use personal information about you.

We are required, under data protection legislation, to tell you what information we hold about you, why we hold it, how we use it and to tell you about your rights.

This notice applies to current and former pupils of the Trust.

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – such as other schools, the local council and the government.

Personal information that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Your contact details – name/address/contact details/unique pupil number
- Your test results, details of your learning and what you have achieved in school
- Your attendance records
- Details of any behaviour issues or exclusions
- Biometric data (catering system use)
- Information about how you use school computers and other IT and communications systems

We may also collect, use, store and share (when appropriate) information about you that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about your characteristics, like your ethnic background, religion, special educational needs/Free school meals eligibility/gender/language
- Information about any medical conditions you have
- Safeguarding information
- Photographs and CCTV images

We may also hold data about you that we have received from other organisations, including other schools and local authorities.

Why we use this data

We use the data listed above to:

- Support pupil learning including using third party providers e.g. Mymaths/Tassomai/Classcharts
- Get in touch with you and your parents or carers when we need to
- Check how you're doing in exams and monitor your progress
- Track how well the school as a whole is performing
- To publish statistics, for example the number of pupils in schools
- Answer your questions and complaints
- Look after your wellbeing
- Make sure our computers and other school systems and equipment are used appropriately, legally and safely
- To meet statutory/legal duties placed upon us for DFE and Government

Use of your personal data in automated decision making and profiling

We will only use your personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for any other reason and that reason is incompatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis that allows us to do so.

Please note that we may process your personal information without your knowledge or consent in compliance with the above rules where this is required or permitted by law.

We don't currently put pupils' personal data through any automated decision making or profiling process. This means we don't make decisions about you using only computers, without any human involvement.

If this changes in the future, we will update this notice in order to explain the processing to you, including your right to object to it.

Use of your personal data for filtering and monitoring purposes

While you're in school, we may monitor what material you access on our computers and other IT and communication systems. We do this so that we can:

- Comply with health and safety law and other laws
- Comply with our policies (e.g. Safeguarding policy, IT Acceptable Use policy)
- Keep our network(s) and devices safe from people who aren't allowed to access them, and prevent harmful software from damaging our network(s)
- Protect your welfare

The lawful basis on which we use this information

We will only collect and use your information when the law allows us to. We need to establish a 'lawful basis' to do this.

Our lawful bases for processing your personal information are:

For the purposes of supporting your learning, monitoring your progress, and meeting the statutory duties placed upon us by the DFE, in accordance with the 'public task' basis – we need to process data to fulfil our official duties as a school as set out here:

- Education Act 1996
- Education Act 2002

- Education (Information about Individual Pupils) (England) Regulations 2013
- GDPR UK

For the purposes of looking after your welfare, health and safety (safeguarding), in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law as set out here:

- KCSIE 2025
- Health & Safety at Work 1974
- GPDR UK

For the purposes of providing catering services and the recording of biometric data to fulfil the needs of that service, in accordance with the 'consent' basis – we will get consent to use your personal data. Similarly, in accordance with the "contract" basis – we need to process personal data to fulfil a contract in managing catering services and meeting the data processing needs of other third party service providers. We will process data to meet our responsibilities under law as set out here:

- GDPR UK

For the purposes of health and safety and safeguarding, in accordance with the 'vital interests' basis – we will process this personal data in a life-or-death situation

Where we're allowed to use your information ('given consent'), you may take this back at any time.

Our basis for using special category data

For 'special category' data (more sensitive personal information), we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have got your explicit consent to use your information in a certain way
- We need to use your information under employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The information has already been made obviously public by you
- We need to use it to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation
- We need to use it for health or social care purposes, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for public health reasons, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have got your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent

- The data concerned has already been made obviously public by you
- We need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation

Collecting pupil information

We will only collect and use your personal information when the law allows us to, as detailed above. While most of the information we collect about you is mandatory (i.e. you have to give us the information), there is some information that you can choose whether or not to provide to us.

Whenever we want to collect information from you, we make it clear whether you have to give us this information (and if so, what the possible consequences are of not doing that), or whether you have a choice.

Most of the data we hold about you will come from you or your parents/carers, but we may also hold data about you from:

- Local councils
- Government departments or agencies
- Police forces, courts or tribunals
- Other schools or trusts
- Department for Education (DfE)

Most data collected and held on pupils is in electronic or paper form. Some examples of other data collection means include biometric data, photographic/video and CCTV.

Biometric Data

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash, we will comply with the requirements of the [Protection of Freedoms Act 2012](#).

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can be allocated a pin number to use for cashless catering.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

Primary schools / Nurseries

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Secondary schools

We will obtain written consent from parents/carers, or pupils aged 18 and over, 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 both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.

- Outside of school by external agencies such as the school photographer, newspapers, campaigns

- Online on our school website or social media pages

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, to ensure they cannot be identified.

CCTV

We use CCTV in various locations around the school sites to ensure it remains safe. We will follow the ICO Guidance for the use of CCTV, and comply with data protection principles.

[CCTV and video surveillance | ICO](#)

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Storing and Retaining pupil data – data protection

We keep personal information about you while you're attending our school. We may also keep it after you stop attending our school, if this is necessary. For details on our retention policy please contact the school.

We have security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, changed, or disclosed (given or told to someone else).

Data protection by design and default

We put measures in place to show that we have integrated data protection in all of our data processing activities, including:

- Appointing a 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

The use of our data sharing application WONDE to provide necessary data sharing agreements to provide assurances on data protection from third party users of data.

At school administration level data protection impact assessment processes/forms are used where necessary to determine data handling needs/risks and apply appropriate measures when purchasing new technologies or considering the processing of high risk data such as special category data. We consider who is requesting the data, the purpose for which the data is required, the level and sensitivity of data (special category) and arrangements in place to store and handle the data. An example of this might include using a new third party data sharing service.

Regularly training members of staff on data protection law and guidance.

Where necessary putting appropriate safeguards in place if we transfer any personal data outside of the UK, where different data protection laws may apply

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 safe when not in use

Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access

Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites

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 policy on acceptable use)

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

AI (Artificial Intelligence)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers are familiar with generative chatbots and other AI driven technologies. We recognise that AI has many benefits and uses in our schools to support learning and administration. However, its use can pose a data loss risk if not used and managed carefully. As with data held in electronic or paper form, the greatest risk is to confidential, sensitive and personal data.

To ensure that all confidential, personal and sensitive data remains secure, no staff/students will be permitted to enter such data into generative AI tools or chatbots.

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 (use of third party to manage confidential waste) and overwrite or delete electronic files. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Who we share pupil information with

Where it is legally required or necessary we routinely share pupil information with:

- schools that you attend after leaving the Trust;
- youth support services (pupils aged 13+)
- Cornwall Council and the sponsoring Local Authority of any students placed with us;
- the Department for Education (DfE);
- NHS, including the School Nurse Team.

We share specific, relevant elements of pupil information with:

- selected educational support providers that improve the quality of education or the efficiency of our provision;
- our legal advisors / courts
- our insurers/ auditors
- the police
- health and social welfare organisations
- survey and research organisations
- voluntary organisations

In addition, we also share data securely with third party software systems or service providers:

- information management systems;
- online payments providers;
- cashless catering systems;
- safeguarding management and reporting systems.
- Online resource services such Classcharts/Schoolscomms/Satchel 1/Tassomai/MyMaths/Sparx/Seneca/SISRA/Insight Tracking (others as required)

Why we share pupil information

We may share pupil personal information with third parties (other organisations) where required by law, where it is necessary for the provision of education, where it is in the data subject's interests for us to do so or where we have another legitimate interest in doing so.

We share pupil information with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information about Individual Pupils) (England) Regulations 2013.

The law requires us to share pupil information with specific authorities, including Children's Social Care and other local agencies, if it is for the purposes of safeguarding.

Information that could be relevant to keeping a child safe will be shared so that informed decisions can be made about a child's welfare in order to keep children safe and to ensure they get the support they need.

The data is transferred securely and held by the Department for Education under a combination of software and hardware controls that meet the current government security policy framework.

The data we share about you with the Department for Education is used for a number of different purposes, including to:

- Help decide the amount of money that our school receives
- Monitor how well the education system is working and how well our school is doing in terms of educating our pupils

- Support research

The information shared with the Department for Education about you could include:

- Your name and address
- Your unique pupil number
- Pupil matching reference numbers
- Details of your gender or ethnicity
- Details of any special educational needs (SEN)
- Details of schools attended
- Absence and exclusion information
- Information relating to exam results
- Information relating to any contact with children's services
- What you have done since finishing school

Please note: this list is not exhaustive.

Once pupils in our school reach the age of 13, we are legally required to pass on certain information to the local authority or youth services provider, which has responsibilities regarding the education or training of 13 to 19 year olds under section 507B of the Education Act 1996. Parents/carers, or pupils if aged 16 or over, can request that only their name, address and date of birth be passed to these agencies by informing the data protection officer (DPO).

National Pupil Database

We have to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the [National Pupil Database](#), which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations, such as organisations that promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on [how it collects and shares personal data](#).

You can also [contact the Department for Education](#) if you have any questions about the database.

How to access personal information that we hold about you

You have a right to make a 'subject access request' to gain access to personal information that we hold about you.

If you make a subject access request, and if we do hold information about you, we will (unless there's a really good reason why we shouldn't):

- Give you a description of it
- Tell you why we are holding it, how we are using it, and how long we will keep it for

- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data (decisions made by a computer or machine, rather than by a person), and any consequences of this
- Give you a copy of the information in an understandable form

You may also have the right for your personal information to be shared with another organisation in certain circumstances.

Your other rights regarding your data

Under data protection law, you have certain rights regarding how your personal information is used and kept safe. For example, you have the right to:

- Say that you don't want your personal information to be used
- Object to the processing of personal data that is likely to cause, or is causing, damage or distress
- Stop it being used to send you marketing materials
- Say that you don't want it to be used for automated decisions (decisions made by a computer or machine, rather than by a person)
- In some cases, have it corrected if it's inaccurate
- In some cases, have it deleted or destroyed, or restrict its use
- Withdraw your consent, where you previously provided consent for your personal information to be collected, processed and transferred for a particular reason
- In some cases, be notified of a data breach
- Make a complaint to the Information Commissioner's Office (ICO) if you feel we have not used your information in the right way
- Claim compensation if the data protection rules are broken and this harms you in some way

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to the use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't have the right to object, but you have the right to withdraw consent

To make a complaint or contact our Data Protection Officer for more information please contact:

Data Protection Officer – Mr Ian Foy – ifoy@smart-trust.net

