



St George's School Harpenden, Academy Trust

PRIVACY NOTICE 2019-20

(How we use personal information)

Pupils and Parents, Alumni, Ex-parents, and Staff

Date of issue: May 2018

Reviewed: October 2019

Approved:

Glossary of key terms

"Data Controllers" means organisations, including schools, that determine how people's personal data is processed and for what purpose.

"Data Subjects" means any living individuals whose data the Data Controller processes.

"Processing" means any action in relation to that personal data, including filing and communication.

"Personal Data" includes everything from which a Data Subject can be identified. It ranges from simple contact details via personnel or pupil files to safeguarding information, and encompasses opinions, file notes or minutes, a record of anyone's intentions towards that person, and communications (such as emails) with or about them.

Some categories of personal data are "special category data" under the GDPR. These comprise data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; data concerning health or data concerning a natural person's sex life or sexual orientation; and biometric data. Extra protection is provided for these data.

St George's School Academy Trust is in charge of personal information: in law this means we are called a "data controller" Our registered office is Sun Lane, Harpenden, Herts, AL54TD, tel 01582 765477, registered in England and Wales 8092358.

This policy is intended to provide information about how the school will use (or "process") personal data about individuals including: its staff; its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

This information is provided in accordance with the rights of individuals under Data Protection Law to understand how their data is used. Staff, parents and pupils are all encouraged to read this Privacy Notice and understand the school's obligations to its entire community.

This Privacy Notice applies alongside any other information the school may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This Privacy Notice also applies in addition to the school's other relevant terms and conditions and policies, including

- any contract between the school and its staff or the parents of pupils
- the school's policy on information security and data protection
- the school's CCTV policy
- the school's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded
- the school's IT policies, including its Acceptable Use policy,

Anyone who works for, or acts on behalf of, the school (including staff, volunteers, governors and service providers) should also be aware of and comply with this Privacy Notice and the school's data protection policy, which also provides further information about how personal data about those individuals will be used.

The Data Protection Officer (DPO) is the Deputy Head, who reports directly to the Headteacher. The DPO is not personally liable for data protection in the school – responsibility sits within the organisation. The DPO can be contacted via admin@stgeorges.herts.sch.uk with the subject line "for attention of DPO".

Anyone who wishes to speak to the school about the way we process personal information can contact the DPO. You can ask for a meeting, or leave a letter at reception or send one by post or email.

The basis on which we process information:

In order to carry out its ordinary duties to staff, pupils and parents, the school may process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation. This information will include student and parent contact details, national curriculum assessment results, attendance information, any exclusion information, where students go after they leave the school and personal characteristics such as ethnic group, any special educational needs and relevant medical information. The school will also use photographs.

St George's has a legitimate interest to hold and use data because:

- The Academy Trust is under a legal obligation to collect the information or the information is necessary for us to meet legal requirements imposed upon us such as our duty to safeguard pupils.

- it is necessary for us to hold and use information for the purposes of our functions in providing schooling and so we can look after all members of our community and promote their welfare and progress. For staff we need data to manage staff in their recruitment and the performance of their contract. This is a function which is in the public interest because everybody needs to have an education. This means we have a real and proper reasons to use personal information.

- We will not usually need your consent to use your information. However, if at any time it appears to us that we would like to use personal data in a way which means that we would need consent then we will explain what we want to do and ask the relevant person for consent. This is most likely to be we are involved in activities which are not really part of our job as an Academy Trust / School but we are involved because we think it would benefit our pupils or other members of our community. The school will generally involve parents in student consent issues even if the student can in law make their own decision.

The school asserts that the following uses will fall within that category of its "legitimate interests":

- For the purposes of pupil admissions (and to confirm the identity of prospective pupils and their parents)
- To provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs
- Maintaining relationships with alumni and the school community, including fundraising activity
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records)
- To enable relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate
- To give and receive information and references about past, current and prospective pupils to/from any educational institution that the pupil attended or where it is proposed they attend and to provide references to potential employers of past pupils

- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school within the school community
- To safeguard pupils' welfare and provide appropriate pastoral care
- To monitor use of the school's IT and communications systems in accordance with the school's IT: acceptable use policy
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's policy on taking, storing and using images of children
- For security purposes, including CCTV in accordance with the school's CCTV policy;
- Where otherwise reasonably necessary for the school's core purposes, including to obtain appropriate professional advice and insurance for the school

TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

This will include by way of example:

- Names, addresses, telephone numbers, e-mail addresses and other contact details
- Characteristics (such as ethnicity, language, medical conditions, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (internal and external exam results, data used to provide you with reports on your progress, academic targets and your progress against them)
- Termly reports and other documents that are made available to students and parents
- Information relating to our Rewards and Consequences policy
- Information to keep people safe (medical, child protection and safeguarding information)
- Information on any Special Educational Needs that relevant people may have
- Post-16 learning information (learning aims, information to assist with UCAS or other post-18 destinations)
- Basic information such as usernames and passwords to allow access IT systems and online learning platforms, tools and eBooks
- Car details (about those who use our car parking facilities)
- Biometric information, which will be collected and used by the school in accordance with the school's biometrics policy. This is stored as a numerical code, not in the form of a stored image e.g. fingerprint. More information on this is in our Data protection policy
- Bank details and other financial information, e.g. about parents who pay boarding fees to the school

- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- Where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's position on taking, storing and using images of children which appears in the information security and data protection policy)

In addition, the school may need to process special category personal data or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may 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 an individual's medical condition where it is in the individual's interests to do so: for example for medical advice, social services, insurance purposes or to organisers of school trips
- To provide educational services in the context of any special educational needs of a pupil
- To provide spiritual education in the context of any religious beliefs
- In connection with employment of its staff, for example DBS checks, welfare or pension plans
- To run any of its systems that operates on biometric data, such as for security and other forms of pupil identification (lockers, lunch etc.) or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care

When the school collects personal information on our forms, we will make it clear whether there is a legal requirement for people to provide it, whether there is a legal requirement on the school / academy trust to collect it. If there is no legal requirement then we will explain why we need it and what the consequences are if it is not provided.

HOW THE SCHOOL COLLECTS DATA

Generally, the school receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual); or collected from publicly available resources.

In the case of staff, during the recruitment process we may receive information about individuals from a previous employer or an educational establishment which that person had previously attended. Individuals will know about this because they will have supplied us with the relevant contact details.

WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

Occasionally, the school will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants) or relevant authorities (HMRC, police or the local authority). For the most part, personal data collected by the school will remain within the school, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records [held and accessed only by the school doctor and appropriate school medical or pastoral support staff or otherwise in accordance with express consent]
- pastoral or safeguarding files.

However, a certain amount of any SEND pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires. In certain contexts, medical and health information about students may need to be widely understood by all those who take responsibility for that young person.

Staff, pupils and parents are reminded that the school is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the Local Authority Designated Officer, NHS, or CAMHS, or the police. The school may need to share information with; "Prevent" teams, courts, our legal advisors, our insurance providers, and providers of HR services. Bodies which might legally require us to share data include the police and Social Services and community health providers who visit the school to complete vaccinations. Boarder students are required to register with a local GP, and your information would be shared with clinicians involved in students' care; this would also apply to all students needing treatment while under our care.

The information disclosed to these people / services will include sensitive personal information. Usually this means information about health and any special educational needs or disabilities. We do this because these people need the information so that they can support individuals. The school will not usually need consent to disclose information. However, if at any time it appears to the school that it would need consent then this will be sought before a disclosure is made. It may be in an individual's vital interests for personal information to be passed to these people or services. The school may seek parent or the individual's consent as a matter of good practice but this is not the same as consent being required from either or both.

Once our pupils reach the age of 13, the law requires us to pass on certain information to Hertfordshire County Council who has responsibilities in relation to the education or training of 13-19 year olds. HCC now discharge many of these activities through Herts for Learning. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent / guardian can request that only their child's name, address and date of birth be passed to Hertfordshire County Council by informing the school. This right is transferred to the child once he / she reaches the age 16. For more information about services for young people, please go to our local authority website

The school does share the following information with Youth Connexions Hertfordshire to identify current students during one to one and in order to track the locations of where students then go):

- Date of Birth
- Address
- Further details supplied if appropriate include: Special Educational Needs and Disabilities, English as and additional language, Child Protection, Children in Need, Collegiate Learning Assessment, Pupil Premium Grant.

The school is required, by law (under regulation 5 of the Education (Information about Individual Pupils) England Regulations 2013, to pass some information about our pupils to the Department for Education (DfE). This is the part of the government which is responsible for schools. This information may, in turn, then be made available for use by the local authority.

The DfE may also share information about pupils that we give to them, with other people or organisations. This will only take place where the law, including the law about data protection allows it.

The National Pupil Database (NPD) is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

The school is required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information about Individual Pupils) (England) Regulations 2013. The school analysis of exam results includes sharing data with the DfE supported platform FFT Aspire.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to National Pupil Database: user guide and supporting information - GOV.UK.

The school will also normally give information about students to parents or their main carer. Where appropriate, the school will listen to student views first. The school will also take family circumstances into account, in particular where a court has decided what information a parent is allowed to have.

St George's School is involved in collaborative delivery with other schools / colleges and learning providers, which include consortium schools (Roundwood Park and Sir John Lawes), Harpenden Musicale (in the case of students who take Music lessons there), the LINKS ESC, and so on. It will include support agencies such as Harpenden Parent Plus and ESTMA. Pupil information may also be shared to aid the preparation of learning plans and use of data to achieve the objectives identified above. Information provided and held for the purpose of school admissions may be shared with local authorities in order to deter and detect fraud.

Where students take part in activities involving external providers, such data will be shared with these providers to enable the activities to take place. These providers include:

- The English Lacrosse Association
- Duke of Edinburgh's Award scheme
- Herts CC Evolve Trip Management System
- The British Council
- The Rugby Football Union
- National Schools Equestrian Association
- English School's Ski Association

Where students are involved in educational visits which require us to send data to providers other than those above, details of those providers are given by those leading the event, and a separate consent to share data is required of the parent (or the child themselves if aged 13 or over).

Should parents and/or students decline to provide data this may restrict our ability to keep people informed of student progress; meet student needs; contact parents in an emergency, and so on. This may prevent a student taking part.

If a student or parent is not willing for student data to be shared with parties who need to process the data so that the student can take part in an extra-curricular programme or activity or trip, then the student is disqualified from that opportunity.

The school Parent and Staff Association, Cecil Grant Trust Fund, The Georgians, and the Alumni Association all work to support the values of the school, its community, and its educational provision. Such limited data will be shared with them which is necessary for them to discharge their role

The school will use data to contact parents and guardians, including by email, text, and other digital means, to inform them about:

- Events involving students
- Parent information events
- Other events in school
- Selected opportunities which we believe may be of interest to them
- Fundraising
- Safeguarding issues or issues of current concern in the community

Some of the organisations we share data with will also be Data Controllers in their own right in which case we will be jointly controllers of your personal data and may be jointly liable in the event of any data breaches.

In the event that we share personal data about pupils with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

Transfer of Records to other Institutions

Where students leave school to another education provider other than at the usual leaving point at the end of year 13, records are transferred to the receiving institution. This includes such records as we are beholden to transfer by law, such as Child Protection records.

The school will provide such information to other education providers that a student might be seeking admission to, be it schools, colleges, or universities. This will not extend to sensitive information at the point where a student is seeking admission. Once a student has gained admission, such information may be transferred if it is necessary to safeguard the student or others at the receiving institution.

The school does not normally transfer student information to a different country which is outside the European Economic Area. This would only happen if a parent lives abroad or if a student moves to a new school abroad. If this happens we will be very careful to make sure that it is safe to transfer your information. We will look at whether that other country has good data protection laws for example, and seek consent if we have any concerns.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

Finally, in accordance with Data Protection Law, some of the school's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

Teaching staff and the school currently use the following app-based means of storing and retrieving data:

- Edulink
- Google Drive
- GCSEpod
- iDoceo
- Edmodo
- Additioapp
- Unifrog
- Snaprevise
- Kerboodle
- Educake
- Survey123
- Everlearner
- Pearson Active Teach
- All-in.org.uk

This list is updated every September; during the year teaching staff may trial other storage platforms as long as they meet appropriate standards of security, with a decision on formal inclusion in this privacy notice at the next review point.

- The boarding houses record information relating to Boarders on “Boardingware”
- Signing in and out records are held on the “Inventry” system
- The school meals system requires data to be held by Cunninghams and “Biostore”
- Payments for a variety of services provided by the school require data to be held on the “Parentpay” system
- Student medical data from September 2018 will be held on “Patient Tracker”, software specifically designed to hold such data securely
- Employee payroll operations require that relevant staff data is sent to SERCO

HOW LONG WE KEEP PERSONAL DATA

The school will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the school. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Data Protection Officer. However, please bear in mind that the school may have lawful and necessary reasons to hold on to some data.

A student may request to have all of their data held by the school deleted following leaving the school at the end of year 13. At the point of such a request the Data Protection Officer would explain the consequences of such an action.

In the case of a student with an Education Health and Care Plan, or a Statement of Special Educational Needs, their school record will be retained until they would reach the age of 80.

Full details of the guidance we follow on retention of data is in an annex to the school Data Protection and Information Security Policy.

YOUR RIGHTS

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the school, and in some cases ask for it to be erased or amended or for the school to stop processing it, but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation should put their request in writing to the DPO.

The school will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is one month in the case of requests for access to information. The school will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the school may ask you to reconsider or charge a proportionate fee, but only where Data Protection Law allows it.

You should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts (though examiners' comments may sometimes be disclosed), nor any confidential reference given by the school for the purposes of the education, training or employment of any individual. Records relating to child protection / safeguarding are not releasable.

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making (see section Whose Rights below). Indeed, while a person with parental responsibility will generally be expected to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child's at law. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf, and moreover (if of sufficient age) their consent or authority may need to be sought by the parent.

Pupils aged 13 are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Children younger than 13 may be sufficiently mature to have a say in this decision. All subject access requests from pupils will therefore be considered on a case by case basis.

Where the school is relying on consent as a means to process personal data, any person may amend this consent at any time (subject to similar age considerations as above). Please be aware however that the school may have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation has been requested).

WHOSE RIGHTS ?

The rights under Data Protection Law belong to the individual to whom the data relates. However, the school will often rely on parental consent to process personal data relating to pupils (if consent is required) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's 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.

In general, the school will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, 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, unless, in the school's opinion, there is a good reason to do otherwise. Note that that school will continue to respond to and interact with a student's parent up until the December 31st following the student leaving the school, unless the student indicates that following their departure they wish their data to be private to themselves.

Parents of pupils who attend academies have a separate statutory right to receive an annual written report setting out their child's attainment for the main subject areas which are taught. This is an independent legal right of parents rather than a pupil's own legal right which falls outside of the GDPR, therefore a pupil's consent is not required even a pupil is able to make their own decisions in relation to their personal data, unless a court order is in place which states otherwise.

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth

certificate or has parental responsibility for the pupil, with whom the pupil lives or whether the pupil has contact with that parent), and also includes non-parents who have parental responsibility for the pupil, or with whom the pupil lives. It is therefore possible for a pupil to have several “parents” for the purposes of education law.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school may be under an obligation to maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example where the school believes disclosure will be in the best interests of the pupil or other pupils, or is required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the schools acceptable use policy and Information Security and Data Protection and the school rules. [Staff are under professional duties to do the same covered under the relevant staff policy.]

DATA ACCURACY AND SECURITY

The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the school of any changes to information held about them.

An individual has the right to request that any inaccurate or out-of-date information about them is erased or corrected (subject to certain exemptions and limitations under Act): please see above.

The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

Where St George's School has material grounds to believe that information is defunct, such a phone number being listed unavailable or an email bouncing back, the school will delete this information speedily.

Data providers in dispute over whether information held by the school is fair and accurate have the right to lodge with the school their divergent information, opinion, or account, and ask that it be held alongside the schools.

QUERIES AND COMPLAINTS

Any comments or queries on this policy should be directed to the DPO using the contact details above.

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the school complaints / grievance procedure and should also notify the DPO (or the Headteacher if the complaint is about the DPO). The school can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

<http://www.hertsdirect.org/services/edlearn/privsch/>

<http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause>

If you are unable to access these websites, please contact the LA or DfE as follows:

Data Protection Team
Information Governance Unit
Room C1
County Hall
Pegs Lane
Hertford
SG13 8DQ

Email: dataprotection@hertscc.gov.uk

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT

Website: www.education.gov.uk

Email: <http://www.education.gov.uk/help/contactus>

Telephone: 0370 000 2288

You can also complain to or seek information from:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

Legal and regulatory framework Various laws underpin this Privacy Notice and are relevant to schools:

The General Data Protection Regulation (from 25 May 2018)

The Data Protection Act 2018 and related legislation (from 25 May 2018, form TBC)

The Privacy and Electronic Communications Regulations 2011 (PECR) (to continue after 25 May 2018 until replaced by the ePrivacy Regulation – form and date TBC)

The Protection of Freedoms Act 2012 (biometrics and CCTV)