

Simon Balle All-through School

Creating tomorrow's citizens today



PRIVACY NOTICE FOR STUDENTS

First Issue:	May 2018
Current Version:	September 2023
Next Review:	September 2024
Committee Responsible:	Board of Trustees

Contents

Introduction	1
Why do we collect and use pupil information?	1
Collecting pupil information	3
Storing pupil data	3
Who do we share pupil information with?	4
Aged 14+ qualifications	5
Why we share pupil information	5
What is different about students aged 13+?	5
Our students aged 16+	6
The National Pupil Database (NPD)	6
Requesting access to your personal data	7
For students in the secondary phase and sixth form	7
Contact	8
Glossary of Terms	9
Changes to this Privacy Notice	10

Introduction

Simon Balle All-through School is required by law to collect and process personal data relating to all of its students. This privacy notice provides you with information about how we collect and process personal data of our students in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Why do we collect and use pupil information?

We collect and use pupil information under section 537A of the Education Act 1996, section 83 of the Children Act 1989, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

We collect and use pupil information under the following lawful bases under the UK General Data Protection Regulation (UK GDPR):

- where we have the consent of the data subject [Article 6 (a)];
- where it is necessary for compliance with a legal obligation [Article 6 (c)];
- where processing is necessary to protect the vital interests of the data subject or another person [Article 6 (d)];
- where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [Article 6 (e)].
- where processing is necessary for our legitimate interests or the legitimate interests of a third party [Article 6 (f)].

Where the personal data we collect about students is sensitive (i.e. special category) personal data, we will only process it where:

- we have explicit consent [Article 9 (2)(a)];
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent [Article 9 (2)(c)]; and/or
- processing is necessary for reasons of substantial public interest, and is authorised by UK law (see section 10 of the 2018 Data Protection Act) [Article 9 (2)(g)].

Please see the Glossary at the end of this privacy notice for definitions of key terms.

We use the pupil data to support our statutory functions of running a school, including but not limited to:

- to decide who to admit to the school;
- to maintain a waiting list;
- to support pupil learning;
- to monitor and report on pupil progress;

- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing;
- for the protection and welfare of students and others in the school;
- for the safe and orderly running of the school;
- to promote the school;
- to provide school trips, wrap-around care and other extra-curricular activities;
- to communicate with parents/carers.

The categories of pupil information that we collect, hold and share include, but is not limited to:

- Personal information (such as name, unique pupil number, address and bank account details);
- Characteristics (such as ethnicity, language, medical conditions and free school meal eligibility);
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Assessment information such as current pupil progress, predicted progress and where appropriate data relating to any assessments, tests or exams students have undertaken;
- Relevant medical information including any conditions or allergies students may have, the need for epi-pens/medication, emergency contact and doctor's details;
- Special educational needs information. This includes information about any particular needs that students have, any funding that is received specifically for SEND, statements of individual need and health care plans;
- Behavioural information, which may include information about students' general classroom behaviour including any awards gained, together with any detentions fixed-term or permanent exclusions they have received;
- Pastoral and safeguarding information, including notes on any home visits undertaken;
- Photographs;
- CCTV images.

From time to time and in certain circumstances, we might also process personal data about students, some of which might be sensitive personal data, including information about criminal proceedings/convictions, information about sex life and sexual orientation, child protection/safeguarding. This information is not routinely collected about students and is only likely to be processed by the school in specific circumstances relating to particular students, for example, if a child protection issue arises or if a pupil is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and/or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

We collect information about students when they join the school and update it during their time on the roll as and when new information is acquired.

As the school has a cashless catering system, we also process biometric data about students. Please see our Data Protection Policy for more details about how we process biometric data.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. Where appropriate, we will ask you (under certain circumstances, see below) or your parents/carers for consent to process personal data where there is no other lawful basis for processing it. For example, where we wish to use photos or images of students on our website or on social media to promote school activities or if we want to ask your permission to use your information for marketing purposes. Parents/carers/students may withdraw consent at any time.

When students are deemed to be old enough to make their own decisions in relation to their personal data, we will also ask the pupil for their consent in these circumstances. This will usually be around the age of 13. Although parental consent is unlikely to be needed, we wish to take a collaborative approach so we will keep parents informed when we are approaching students for consent up to the age of 18. Students with the maturity to make their own decisions about their personal data may withdraw consent if consent has previously been given.

In addition, the school also uses CCTV cameras around the school site for security purposes and for the protection of staff and students. CCTV footage may be referred to during the course of disciplinary procedures (for staff or students) or investigate other issues. CCTV footage involving students will only be processed to the extent that it is lawful to do so. Please see our CCTV Policy for more details.

Storing pupil data

We hold pupil data securely and have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. Access to information is limited to those who have a business need to know it and who are subject to a duty of confidentiality. A significant amount of personal data is stored electronically, for example, on our MIS database. Some information may also be stored in hard copy format.

Data stored electronically may be saved on a cloud based system which may be hosted in a different country.

Personal data may be transferred to other countries if, for example, we are arranging a school trip to a different country. Appropriate steps will be taken to keep the data secure.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach involving your data where we are legally required to do so.

When a pupil moves to another educational setting or school phase, the vast majority of information that we hold will move to that setting, although we may need to retain a certain amount of personal data, as laid out in our Data Retention Policy and Schedule.

Where we act as the final setting in a pupil's education, we are required to retain some personal information for a period after they have left. Typically that information will be retained until they reach the age of 25, after which it may be archived or securely destroyed. There may be reasons for retaining data longer than this, which are laid out in our Data Retention Policy and Schedule.

Who do we share pupil information with?

We routinely share pupil information with:

- schools that students attend after leaving us;
- our local authority Hertfordshire County Council;
- a pupil's home local authority (if different);
- commissioned providers of local authority services e.g. HFL Education
- the Department for Education (DfE);
- school governors/trustees;
- exam boards

From time to time, we may also share pupil information with other third parties including, but not limited to, the following:

- external contractors that provide services to the school such as catering, cashless payment systems, payroll etc.
- the Police and law enforcement agencies;
- NHS health professionals including the school nurse, educational psychologists, speech and language therapists etc.;
- education welfare officers;
- courts, if ordered to do so;
- the National College for Teaching and Learning;
- the Joint Council for Qualifications;
- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances;
- our HR providers, for example, if we are seeking HR advice and a pupil is involved in an issue;
- UCAS
- our legal advisors;
- HMRC and the Local Government Pension Scheme (LGPS) when students are employed by the school

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

We may also share pupil data with a number of providers of software tools which may be used to: support pupil learning; monitor and report on pupil attainment and progress; deliver the educational curriculum; ensure the safety and wellbeing of students; communicate with

parents; or to carry out other operational processes to support our core activities as a public authority, under Article 6(e) of the UK GDPR. A full list of these providers is available on request. These providers act as data processors on our behalf, and are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow them to use your personal data for their own purposes, and we only permit them to process your personal data for specified purposes and in accordance with our instructions.

In the event that we share personal data about students with third parties or data processors, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data. Where necessary, we will carry out a Data Protection Impact Assessment (DPIA) to assess any risks involved.

Aged 14+ qualifications

For students enrolling for post 14 qualifications, the information you supply is used by the Learning Records Service (LRS). The LRS issues Unique Learner Numbers (ULN) and creates Personal Learning records across England, Wales and Northern Ireland, and is operated by the Education and Skills Funding Agency, an executive agency of the Department for Education (DfE). The LRS will give us a pupil's ULN and may also give us details about the pupil's learning or qualifications. For more information about how your information is processed, and to access your Personal Learning Record, please refer to the [LRS Privacy Notice](#).

Why we share pupil information

We do not share information about our students with anyone without consent unless the law allows us to do so.

We share students' data 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 students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the data collection requirements placed on us by the Department for Education (for example, via the school census), please refer to the [DfE guidance](#).

What is different about students aged 13+?

Once our students reach the age of 13, we also pass pupil information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision

of youth support services will be shared. This right is transferred to the child/pupil once they reach the age 16.

Data is securely transferred to the youth support service via encrypted email and is stored electronically and held in accordance with the service's data retention schedule.

Our students aged 16+

We will also share certain information about students aged 16+ with our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers;
- youth support services;
- careers advisers.

Data is securely transferred to the youth support service via encrypted email and is stored electronically and held in accordance with the service's data retention schedule.

For more information about services for young people, please visit our [local authority website](#).

The National Pupil Database (NPD)

The NPD is owned and managed by the DfE and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the DfE. 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.

We are required by law to provide information about our students 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 Students) (England) Regulations 2013.

To find out more about the NPD, please refer to the [NPD website](#).

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;

- the level and sensitivity of data requested; and
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please refer to the [DfE's website](#).

For information about which organisations the department has provided pupil information, (and for which project), please refer to the [DfE's website](#).

To contact DfE, please visit their [contact page](#).

Requesting access to your personal data

For students in the primary phase: Under data protection legislation, parents and students have the right to request access to information about them that we hold ("Subject Access Request"). Where a child does not have the maturity to make their own requests for personal data, parents may do so on their behalf in a primary school setting. To make a request for your child's personal data, or be given access to your child's educational record, please contact the Data Protection Officer (DPO), Will Davies (dpo@simonballe.herts.sch.uk); although any written request for personal data will be treated as a Subject Access Request.

For students in the secondary phase and sixth form

Under data protection legislation, students, and in some circumstances, parents, have the right to request access to information about them that we hold ("Subject Access Request"). From the age of 13, we generally regard students as having the capacity to exercise their own rights in relation to their personal data. This means that where we consider a pupil to have sufficient maturity to understand their own rights, we will require a Subject Access Request to be made by the pupil and not their parent(s) on their behalf. This does not affect any separate statutory right parents might have to access information about their child.

Subject to the section below, the legal timescales for the School to respond to a Subject Access Request is one calendar month. As the School has limited staff resources outside of term time, we encourage parents/students to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible. For further information about how we handle Subject Access Requests, please see our Data Protection Policy.

Parents of students 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 UK GDPR, therefore a pupil's consent is not required, even if 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.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of our data protection responsibilities.

We will always seek to comply with any requests regarding your rights, however please note that we may still be required to hold or use your information to comply with legal duties.

For further information about your rights, including the circumstances in which they apply, see the [guidance](#) from the Information Commissioner's Office (ICO) on individuals' rights under the UK GDPR.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the [Information Commissioner's Office](#).

Contact

You can contact the Information Commissioner's Office on 0303 123 1113 or via email or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

If you would like to discuss anything in this privacy notice, please contact the Trust Data Protection Manager, Haydn Walsh (walshh@simonballe.herts.sch.uk) or the DPO, Will Davies (dpo@simonballe.herts.sch.uk).

Glossary of Terms

Biometric Data

Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics which allow or confirm the unique identification of that person, such as fingerprints.

Consent

Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the Processing of Personal Data relating to them.

Data Controller

Exercises overall control over the purposes and means of the Processing of personal data.

Data Processor

Acts on behalf of, and only on the instructions of, the relevant Controller.

Data Protection Officer (DPO)

Monitors internal compliance of an organisation, informs and advises on data protection obligations.

Data Subject

Data Subjects for the purpose of this policy include all living individuals about whom we hold Personal Data.

Data User

Data Users include employees, volunteers, governors whose work involves using Personal Data.

Information Commissioner's Office (ICO)

Independent public body responsible for ensuring compliance with the UK's data protection regulations by providing guidance, investigating breaches of the regulations and dealing with complaints.

Parent

Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child

Personal Data

Any information relating to an identified or identifiable natural person, which could be as simple as a name or a number, or which could include other identifiers e.g. date of birth, photo, IP address etc.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

Privacy by Design

Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR

Processing

Any operation which is performed on Personal Data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, erasure or destruction.

Special Category Data

Personal Data revealing or concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health and sexual orientation.

Subject Access Request (SAR)

A formal request from a data subject for information, including Personal Data, which an organisation holds about them.

Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.