



Privacy Notice - Students

In the process of teaching and looking after our students we collect, hold and share lots of personal information. This document aims to describe this data, explain what we do with it, and outline your data protection rights.

We promise to ensure that this personal information is processed fairly, is correct, is stored safely, and is kept for no longer than needed.

This Privacy Notice also covers the activities of ImberLink, the charity we run to collect donations from Parents and Friends of the school. The money raised is used to invest in improving the education of our students by providing items not normally covered by our government funding. ImberLink is a registered charity (no. 271227).

Who should I contact about data protection issues?

We have chosen a member of staff, Mr. Alex Melmoe, to have responsibility for data security – he is our Data Protection Officer. One of our Governors, Miss Michelle Brooks, oversees Alex and makes sure he's doing the job properly. If you want to talk about your personal information, they can be contacted via e-mail at dataprotection@imberhorne.co.uk or via the school switchboard on 01342 323562.

The Student information we collect, hold and share; what we do with it, and why we do it

- **Personal Information**
(things like name, date of birth, address, contact details, unique pupil number)
- **Characteristics**
(things like ethnicity, language, nationality, country of birth, religion)
Apart from helping people that don't speak English, we don't use it to treat any individuals in a different manner to anyone else – sometimes we'll even use it to make sure we don't.
- **Parent/Carer Information**
(things like name, address, contact details, relationship to student)
We store this information in order to communicate with Parents & Carers about their children and school life.
- **Student ID Photographs**
An official school photographer will take a photograph of each student once per year. We use these to identify students - as faces are often more memorable than names. We keep the most recent photograph until the student is 25, and previous versions until they leave.
- **Photographs of Students**
From time to time we may take photographs of students engaged in school activities, which we may publish in printed publications, on our website, or on our social media pages. We will never publish named photos of students unless we've asked first. Such photos may be kept until the student is 25, but will probably be deleted well before then.
- **Attendance Information**
(lessons and sessions attended, number of absences and absence reasons)



Privacy Notice - Students

- **Medical Information**
(details of any medical problems a student has and how we need to deal with these problems)
We keep medical information that parents/carers have given us to protect the vital interests of the student.
- **Free School Meals Eligibility**
(Whether West Sussex County Council have told us the student can have Free School Meals)
We use it to tell our canteen tills when to give students free meals, and we also use it to see what impact free schools meals have on these students.
- **Behaviour and Achievement information**
(details of good and bad things a students has done, including details of any punishments such as detentions and/or exclusions)
We mainly use this information to reward students for good behaviour, sometimes we use it to punish students for poor behaviour. We also use it to keep an eye on the achievements and behaviour of our students, and to look for patterns to allow us to improve.
- **Student Marks**
(marks given for work during a course)
We keep these for one year after the school year the marks were given in.
- **Formal Assessment and Examination Results**
(results from end of unit/course assessments/tests and external exams)
- **Any special needs or disabilities**
We use this information to cater for the needs of the student concerned and ensure they receive education that is appropriate for them.
- **Students' previous schools and details of where students go after they leave us**
- **Details of any Child Protection concerns**
We use this information to protect the vital interests of an individual – ensuring that the student concerned receives adequate care.
- **Cashless Catering purchase & top-up history**
To run the cashless catering system in the canteen we need to know how much money is on each student's account and what has been spent – this is necessary to provide the service. We look at daily sales totals, and how many Free School Meals have been taken, but don't use the data for anything else. We delete this at the end of the school year after the year that the student leaves to allow us to deal with any queries.
- **Biometric Fingerscans**
When a student starts with us we ask for permission to store their Biometric Fingerscan. The form asks each parent and the student whether or not we can take a fingerscan – we need at least one parent and the student to say yes before we take a fingerscan. If we have a single no from either parent or the student we won't store the fingerscan, and will issue a card instead. We delete these at the end of the school year that the student leaves.
- **Household income details (if a 16-19 Bursary has been applied for)**
If a student applies for a 16-19 bursary we need to know the income of their household to decide whether or not they can have a bursary. We keep this for 7 years after the financial year the application was made in.

Privacy Notice - Students

- **Times and computers used to logon to school network**

When someone logs on to or off of our school network, or uses Remote Access, we record their username, computer name, and date and time they did so. We use this in cases of network abuse, data loss, or damage to equipment, protecting these legitimate interests. We keep this for 2 years.

- **History of websites accessed from the school network**

When someone uses the school network to visit a website we record their username, computer IP address, and the website they have visited. We do this because we have a Legal Obligation to keep our students safe online and to prevent radicalisation. We keep this for 3 months.

- **Mobile phone IMEI and serial numbers (where ActiveSync has been configured)**

If a student connects their mobile phone, a tablet, or similar device to ActiveSync – the system that puts their e-mail and calendar on the device – we record the Serial Number and IMEI number of the device concerned. This allows the student, or our IT Support Team, to remotely wipe or disable the device if lost or stolen, protecting these legitimate interests. In some cases we use the data to reunite lost devices with their owners. We delete this 90 days after the student leaves.

- **Times of Site access (if Access Controlled gates used)**

Sixth Form students can enter and leave our school site via a set of electronic gates at any time during the school day. Each time they do so we record the date and time they opened the gate and the gate reader they used. We do this so we know who is on site and to protect our wider student community. We delete this when the student leaves.

- **CCTV Footage**

Our CCTV system is used for Site Security (detecting and deterring crime), Safeguarding (monitoring who comes in and off site), Behaviour Management, and Vandalism Prevention (people damaging property of others). We do this as we have a legal obligation to ensure the safety of our students, to uphold acceptable behaviour, and to protect the property of the school and others. A limited number of staff are allowed to see the footage, and we do not use the footage for any other reason. We retain footage for 48 days.

Retention of data

Unless we've said otherwise in the previous section, we keep student data until the student reaches 25 years old, mainly because the law says we have to.

Once we reach the time to dispose of the data electronic data is deleted and any paper records are shredded using a company that performs shredding on-site.

Our legal basis for processing personal data

The current data protection laws require us to have a "legal basis" for processing personal data. As we are a public body, the vast majority of our data is processed because the law says we have to (i.e. to comply with our legal obligations) and to enable us to perform tasks carried out in the public interest.

Any categories of data where this is not the case have their "legal basis" listed in their descriptions above.



Privacy Notice - Students

How we use the information we store

We collect and hold personal information relating to our students and those involved in their care. We usually collect this directly from the student or parent, but we may also receive information from previous schools, the local authority and/or the Department for Education (DfE).

We use this personal data to:

- support our students' learning
- support our students' welfare
- monitor and report on their progress
- provide appropriate pastoral care
- assess the quality of our services
- administer the charitable functions of ImberLink
- process any complaints
- protect vulnerable individuals
- prevent and detect of crime

Who we share student information with

We may share student information with:

- Schools that a student attends after leaving our school
- The Department for Education (DfE)
- Youth Support Services
- Clinical Commissioning Groups (part of the NHS)
- The National Pupil Database (NPD)
- West Sussex County Council (the local authority)
- Social Services
- Police, Fire and Rescue Service, Ambulance Service and other emergency or enforcement agencies
- Employers offering work experience to students
- Joint Council for Qualifications (JCQ) / Examination Boards
- A partner school if it is agreed that a student will be educated there as part of a managed move arrangement
- Alternative education providers if it is agreed that a student will be educated off-site by them

We don't share information about our students without consent unless the law and our policies allow us to do so. Full details of who we share data with and why can be found at the back of this document.

Your rights

Under the current GDPR data protection regulations, we have to inform you that you have the following rights. Should you wish to exercise any of these rights please contact our Data Protection Officer – details on the first page of this document.

- **The right of access**

Being able to get a copy of the data we hold. Some data can be accessed through the MyChildAtSchool website and app. You can also contact us to request a copy of the data we hold – called a “Subject Access Request”. We have to get back to you as soon possible as we can’t take longer than a month to provide the data.

- **The right to rectification**

Being able to ask us to fix mistakes – although please note that some data can be updated by completing a “Data Collection Sheet” in the MyChildAtSchool website and app.

- **The right to erasure**

Have information we hold deleted.

- **The right to restrict processing**

Which means we can still hold the data, but can’t use it.

- **The right to object**

Where we process data on the grounds of consent you are free to withdraw that consent at any time. You also have the right to object to processing of personal data that is likely to cause, or is causing, damage or distress

Note that there are circumstances when the above rights don't apply, like when a law says we need to hold certain pieces of information, or if not processing the data places a student in danger.

Data Protection Complaints

If you are unhappy with the way your request has been handled, you may wish to ask for a review of our decision by contacting our Data Protection Officer.

If you are not content with the outcome of the internal review, you may apply directly to the Information Commissioner (the Government Body responsible for data protection) for a decision. Generally, the Information Commissioner cannot make a decision unless you have exhausted our internal review procedure.

You can log a complaint with the Information Commissioner online at <https://ico.org.uk/concerns/>



Who we share student information with and why

Department for Education (DfE)

The law says we have to share student data with the Department for Education (DfE) and West Sussex County Council, this data sharing underpins school funding and educational attainment policy and monitoring. The part of law that says this is section 3 of The Education (Information About Individual Pupils) (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) go to

<https://www.gov.uk/education/data-collection-and-censuses-for-schools>

Youth Support Services

Once students reach the age of 13, the law requires us to pass student information to the local authority and / or the provider of Youth Support Services in the area 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
- youth support services
- careers advisers

A parent or carer can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the student once they reach the age 16.

For more information about services for young people, please visit www.westsussex.gov.uk

Clinical Commissioning Groups (CCGs)

We are required, by law, to pass certain information about our students to CCGs.

CCGs use information about students for research and statistical purposes, to develop, monitor and evaluate the performance of local health services. These statistics will not identify individual students. It is necessary for certain health information about children (for example, such as their height and weight) to be retained for a certain period of time (designated by the Department of Health) and requires these CCGs to maintain children's names and addresses for this purpose. CCGs may also provide individual schools and Local Authorities (LAs) with aggregated health information which will not identify individual children.



Privacy Notice - Students

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education 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 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.

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 Pupils) (England) Regulations 2013.

To find out more about the NPD, go to:

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

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 Department 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
- the arrangements in place to store and handle the data

To be granted access to student 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 visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided student information, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact the DfE visit: <https://www.gov.uk/contact-dfe>



Privacy Notice - Students

Local Authority - education and training

We are required, by law, to pass certain information about our students to local authorities.

The LA holds information about young people living in its area, including about their education and training history. This is to support the provision of their education up to the age of 20 (and beyond this age for those with a special education need or disability). Education institutions and other public bodies (including the Department for Education (DfE), police, probation and health services) may pass information to the LA to help them to do this.

The LA shares some of the information it collects with the Department for Education (DfE) to enable them to produce statistics, assess performance, determine the destinations of young people after they have left school or college, and to evaluate Government funded programmes.

The LA may also share information with post-16 education and training providers to secure appropriate support for them. They may also share data with education establishments which shows what their pupils go on to do after the age of 16.

If you want to see a copy of information about you that the LA holds, please contact the Data Protection Officer: FOI@westsussex.gov.uk

Social Services

In order to comply with our statutory safeguarding duties we are required, by law, to pass certain information about our students to local authorities. Information will only be shared where it is fair and lawful to do so.

If you want to see a copy of information about you that the LA holds, please contact the Data Protection Officer: FOI@westsussex.gov.uk

Police, Fire and Rescue Service, Ambulance Service and other emergency or enforcement agencies

In order to comply with our duty of care to students, our statutory safeguarding duties and our obligations in respect to the prevention and detection of crime, we may also share personal data with other statutory and partnership agencies.

Employers offering Work Experience to students

If students are offered a Work Experience placement with a company we may pass a small amount of personal information to the Employer concerned. This will be limited to the name and age of the student, summary medical and/or allergy information and parent/carer contact details, to be used in case of an emergency.

We will ask for permission before passing such data to the Employer.



Privacy Notice - Students

Joint Council for Qualifications (JCQ) / Examination Boards

Once a student is enrolled on a course that is externally assessed or examined we will share certain items of information about them with the relevant examination board and/or JCQ – the body that co-ordinates examinations – to enable them to administer the qualifications. We do this to enable us to carry out our duties which are in the public interest.

In most cases the data transferred will be limited to the name(s), date of birth, gender, Unique Candidate Identifier (UCI), and Unique Learner Number (ULN) of a student. In some cases additional information, including sensitive data relating to health, may be shared to support applications for access arrangements and reasonable adjustments and/or special consideration.

After the examination/assessment, the examination board will share with us the results achieved by the student.

Personal data within candidates' work will be collected and processed by an awarding body for the purposes of marking, issuing of examination results and providing candidates with access to post-results services. Examination results will be retained by the awarding body for a minimum of forty years.

In order for an awarding body to achieve this, some personal information may be transferred to third parties such as examiners, who may in some instances, reside outside the European Economic Area.

Awarding bodies may be required to provide a candidate's personal data to educational agencies such as DfE, WG, DE, The Skills Funding Agency, regulators, HESA, UCAS, Local Authorities, EFA and Learning Records Service (LRS). Additionally, candidates' personal data may be provided to a central record of qualifications approved by the awarding bodies for statistical and policy development purposes.

JCQ's full privacy notice can be found here: <https://www.jcq.org.uk/exams-office/information-for-candidates-documents/information-for-candidates---privacy-notice>

External Service Providers

We may use outside companies to provide services to students and parents on behalf of the school.

Where we do this we shall ensure that they share our commitment to data security, and that they only receive data required to perform the service they are providing. We won't pass any sensitive personal data outside of the European Union.

Such service providers include:

- ParentPay – used to provide online payments
- Bromcom – used to manage student records and allowing parents & students access to student data
- Microsoft Office365 (student names only)
- Google G Suite (student names only)
- Adobe (student names only)
- CPOMS – Child Protection and Safeguarding system
- Accessit – Library Management System
- JP Photographic – School Photographer
- Greater Brighton Metropolitan College Work Experience System – used to arrange work experience placements for students

**Summary of Changes to this Document**

From time to time we make small changes to this document to ensure it continues to describe how we process your data accurately. The table below summarises changes we have made.

Date	Author	Changes
10/01/23	AJM	Updated uses of CCTV.
10/01/23	AJM	Updated External Service Providers list.
10/01/23	AJM	Changed Data Protection Governor due to resignation of previous post holder.
16/09/21	AJM	Altered CCTV Footage retention period from "We retain footage of the perimeter of the Imberhorne Lane site for 14 days, and all other footage for 48 days" to "We retain footage for 48 days" following CCTV system upgrade.
16/09/21	AJM	Updated External Service Providers list.
31/03/21	AJM	Changed Data Protection Governor due to resignation of previous post holder.
17/09/18	AJM	Corrected Bursary description on page 2 from 11-19 Bursary to 16-19 Bursary.
04/06/18	AJM	Changed Data Protection Governor due to resignation of previous post holder.