



## Privacy Notice - Staff

In order to run our school we need to hold a quantity of staff 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.

### 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, Mrs. Celia Wilson, 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](mailto:dataprotection@imberhorne.co.uk) or via the school switchboard on 01342 323562.

### The Staff 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, national insurance & teacher numbers)*
- **Characteristics**  
*(things like ethnicity, language, nationality)*  
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.
- **Next of Kin/Emergency Contact Information**  
*(things like name, address, contact details)*  
Knowing this will help us protect the vital interests of a member of staff in the case of an emergency.
- **Staff ID Photographs**  
We use these to identify staff and to produce staff ID badges as part of our safeguarding duties. We keep the most recent photograph for 7 years after you leave our employment, and don't keep any previous versions.
- **Photographs of Staff**  
From time to time we may take photographs of staff whilst 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 staff unless we've asked first. Where such photos contain only staff, we will retain them for up to 5 years after the event concerned. If photos contain students, they may be kept until the students involved are 25, but will probably be deleted well before then.
- **Contract Information**  
*(things like start dates, hours worked, post, role and salary information)*
- **Work Absence Information**  
*(things like number of absences and reasons)*
- **Performance Information**  
*(things such as records of capability and/or disciplinary matters)*
- **Appraisal Records**  
We keep these for 5 years after the academic year it relates to.

## Privacy Notice - Staff

- **Qualifications Information**  
*(including subjects taught if relevant)*
- **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 account and what has been spent – this is necessary to provide the service. We look at daily sales totals, but don't use the data for anything else. We delete this at the end of the school year after the year that the member of staff leaves to allow us to deal with any queries.
- **Biometric Fingerscans**  
When a member of staff starts with us we ask for verbal permission to store their Biometric Fingerscan – if they object, we don't take a fingerscan. We delete these at the end of the school year that the member of staff leaves.
- **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 member of staff 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 member of staff, 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 7 days after the member of staff leaves.
- **Times of Site access (if Access Controlled gates used)**  
Staff 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 member of staff leaves.
- **CCTV Footage**  
Our CCTV system is used for Site Security (detecting and deterring crime), Safeguarding (monitoring who comes in and off site), and Vandalism Prevention (people damaging property of others). We do this as we have a legal obligation to ensure the safety of our staff and students, 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 of the perimeter of the Imberhorne Lane site for 14 days, and all other footage for 48 days.

## Retention of data

Unless we've said otherwise in the previous section, we keep staff data for seven years after the member of staff leaves our employment. 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.



## Privacy Notice - Staff

### 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.

### How we use the information we store

We process personal data relating to those we employ to work, or otherwise engage to work, at our School for:

- employment purposes
- to enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- to assist in the running of the School
- to enable individuals to be paid

The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring
- supporting the work of the School Teachers' Review Body
- protecting vulnerable individuals
- the prevention and detection of crime

### Who we share staff information with

We may share staff information with:

- West Sussex County Council (the local authority)
- the Department for Education (DfE)
- Health Management (WSSCC's Occupational Health Contractor)
- Police, Fire and Rescue Service, Ambulance Service and other emergency or enforcement agencies

We don't share information about our staff 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. You can 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.*
- **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 staff information with and why

#### Local Authority

We share staff information with West Sussex County Council (our Local Authority) – they are the employer of our staff and need access to certain items of data to enable them to manage payroll, pensions and such like. This allows us to carry out our duties which are in the public interest.

We also have to share certain information with them by law - the part of law that says this is section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and its amendments.



## Privacy Notice - Staff

### Department for Education (DfE)

The law says we have to share staff data with the Department for Education (DfE). This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure, as well as the assessment of educational attainment. The part of law that says this is section 5 of The Education (Supply of Information about the School Workforce) (England) Regulations 2007 and its amendments.

The DfE collects and processes staff personal data from us. We are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005 – this is a requirement for all state funded schools.

To find out more about the data collection requirements placed on us by the Department for Education go to

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

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal 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 securely store and handle the data

To be granted access to school workforce information, organisations must comply with its 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>

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

### Health Management

Health Management provide Occupational Health Services for West Sussex County Council. Should the need arise for us to ask them to provide Occupational Health advice for a member of staff we may need to share some personal information with them. We will only share such information with the permission of the member of staff concerned.



## Privacy Notice - Staff

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

In order to comply with our duty of care to students and staff, 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.

### External Service Providers

We may use outside companies to provide services to staff, 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
- SIMS Learning Gateway/SIMS Parent – allowing parents access to student data
- Microsoft Office365 (student & staff names only)
- Google G Suite (student & staff names only)
- CPOMS – Child Protection and Safeguarding system
- MINTclass – Class Seating Planner
- Eclipse.net – Library Management System
- JP Photographic – School Photographer

### 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
04/06/18	AJM	Changed Data Protection Governor due to resignation of previous post holder.