



The Crypt School Data Privacy Notice for Staff

The Crypt School is the Data Controller for the use of personal data in this privacy notice

Introduction

This notice summarises why we collect personal data about people working for the School; how we use that data; and your rights in relation to the personal data the School holds about you.

"Personal data" means data that relates to a living individual who can be identified. It includes names, addresses and other contact details, photographs, identification numbers or online identifiers and location data.

The Crypt School is the data controller of the personal information you provide to us. This means the School determines the purposes for which, and the manner in which, any personal data relating to staff is to be processed. In some cases, your data will be outsourced to a third party processor.

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by the School's employees and service providers in the performance of their duties.

The Crypt School's Data Protection Officer is Gloucestershire County Council. Their role is to oversee and monitor the School's data protection procedures, and to ensure that they are compliant with the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. Their contact details are schoolsdpo@gloucestershire.gov.uk

What data is collected?

The categories of school personnel information that we collect, hold and share (with appropriate people when required) include:

- Personal Information (such as name, date of birth, employee or teacher number, national insurance number, address and contact details, address history and proof of identity)
- Special categories of data, including personal characteristics information such as ethnicity, health and disability information and biometric data used for the site security and cashless catering payment systems

- Contract information (such as start dates, hours worked, post, roles, salary and pension information)
- Work absence information and annual leave (such as number and dates of absences and reasons, special leave)
- Qualifications (and, where relevant, subjects taught), skills, experience and employment history with dates
- References
- Documents to support an Enhanced Disclosure and Barring Service application, such as copies of Passports, Bank statements, Birth and Marriage Certificates
- Medical and health information, including disability for which the organisation needs to make reasonable adjustments
- Photographs (for example, staff passes, staff photos for website and noticeboard)
- CCTV footage
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- Assessments of your performance, including performance improvement plans and related correspondence
- Data concerning your use of the School's information and communication system
- Bank account details for payroll
- In case of emergency, next of kin data or other contact details
- Driving licence data for mini bus drivers.

How we collect your information

We collect this information in a variety of ways. For example, data is collected through application forms; obtained from your passport or other identity documents; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments. In some cases, we collect personal data about you from third parties (e.g. references supplied by former employers or information from Disclosure Barring Service checks). Whilst the majority of personal information you provide to us is mandatory, some of it is provided to us on a voluntary basis with your consent. We will inform you whether you are required to provide certain personal information to us or if you have a choice in this and will make it clear how you can withhold or withdraw your agreement (you may also email the Compliance Officer at foi@crypt.gloucs.sch.uk to do this).

Why do we collect and use information about you?

The Crypt School holds the legal right to collect and use staff personal data.

We use your data to:

- Enable individuals to be paid and comply with statutory deductions
- Meet our obligations to members of both Teachers' and Local Government Pension Schemes
- Conduct safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective attendance and performance management
- Contact your next of kin/emergency contacts in the event of an emergency

- Inform the development and implementation of effective and fair recruitment and retention policies
- Ensure business continuity (e.g. contacting you or family members if you are absent)
- Maintain a secure environment for pupils and staff, including through CCTV
- Maintain a secure ICT system, including through monitoring its use by you
- Enable relevant bodies to monitor or investigate the School's performance
- Enable equalities and equal opportunities monitoring
- Inform our recruitment and retention policies and financial planning
- Support learning through use of educational applications
- Provide information about the School via its website and social media
- Provide prospective employer references at your request
- Support the work of the School Teachers' Review Body (Regulatory Body)
- Meet the requirements of the law regarding data sharing and other legal obligations placed on us by the Department for Education (DfE), including those in relation to:
 - The school workforce census, which is a statutory requirement on schools by virtue of regulations made under sections 113 and 114 of the Education Act 2005
 - Keeping Children Safe in Education (which sets out rules for schools in order to keep pupils safe and promote their welfare)

Use of your personal data for filtering and monitoring purposes

School systems and users are protected by security, filtering and monitoring services. Your use of school devices and systems (including the school Wi-Fi), regardless of time, location or connection, including encrypted content, can be monitored and/or viewed by the relevant authorized staff members. Activity on school accounts on any device may be viewed by the relevant authorized staff. All devices using the school Wi-Fi connection for internet access, and off-site school-owned devices, may be filtered. We do this so that we can:

- Comply with *Keeping Children Safe in Education*, health and safety and other legal obligations
- Comply with our policies
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)

The lawful basis on which we process data

Personal information is collected from you in order to meet and discharge our contractual obligations and statutory duties as your employer. If you fail to provide the personal information requested, amongst other things we may not be able to provide you with employment or a service for which you may be entitled/have requested.

We will only use your information when the law allows us to. We need to establish a 'lawful basis' to do this. The lawful bases we rely on for processing your information are:

- "Public task" – processing the data is necessary to carry out our requirements and responsibilities as a school

- “Vital interests” – the processing is necessary to protect someone’s life
- “Contract” – the processing is necessary for our contract with you
- Consent – you have given clear consent to process your personal data for a specific purpose
- “Legal obligation” – to satisfy our legal obligations and statutory duties as your employer

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the School’s use of your data.

Our basis for using special category data

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

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

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

Storing personal data

We hold your data securely on our school network (including the School’s email system), external servers (cloud storage) and the IT systems of the School’s HR, Finance and Payroll system providers (Every HR by IRIS, IRIS Financials and Dataplan Education by IRIS), who act as data processors on behalf of the School. Personnel files in hard copy are stored in locked filing cabinets. We make sure that people only have access to data that they need for their job. Access to any sensitive personal data is strictly restricted to only those who need to see it.

We normally keep staff personnel records information for 7 years from the date of termination of employment. Records relating to safeguarding cases are kept until the individual’s normal retirement age or 10 years from the date of the allegation (whichever is the longer). Payroll paper records are retained for 14 years purely for pensions historic information and enquiries. After that,

your record is disposed of securely. We use a company with special authorisation to destroy paper records of personal data.

CCTV images are destroyed after 30 days unless they are required in relation to a specific incident. Applications for employment are destroyed after six months from the date of interviews. Accident/injury at work records are retained for at least 4 years from the date of incident and then reviewed for retention or secure disposal.

Will your information be shared and why?

The Crypt School routinely shares personal information with:

- our local authority, Gloucestershire County Council (GCC) and the Department for Education (DfE)
- the Department for Work and Pensions and the National Statistics Office
- Bromcom, The Safeguarding Company Ltd, Every HR by IRIS, IRIS Financials and Dataplan Education by IRIS, who provide software that we use to manage school and employment data. Data is stored on cloud servers and accessed by those companies only as required by the school
- EXA and Securus (for internet, filtering and monitoring services)
- Support staff only: AVC Wise (My Money Matters), for the purpose of advertising the availability of, and administering, additional voluntary pension contributions.

We do not share information about our staff with anyone without consent unless the law and our policies allow us to do so.

We are required to share information about our school employees with the Department for Education under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments. More information about how the DfE uses school workforce personal data is set out in the Annex.

We may also share your information with the Police, courts, tribunals and regulatory authorities.

Transferring data internationally

Where we transfer personal data to another country, we will do so in accordance with data protection law.

Requesting access to your personal data

Under data protection law, you have the right to request access to information about you that we hold. To make a request for your personal information, we ask that you do so in writing on a Data Subject Access Request form, which is available on the School website (Policies and Forms) or from the School Office. Submitting your request using the form enables us to process your request more efficiently, but you may also make a request verbally or by email, for example.

Depending on the lawful basis above, you also have the following rights:

- the right to be informed about the collection and use of your personal data – this is called ‘right to be informed’
- the right to ask us for copies of personal information we have about you – this is called ‘right of access’, this is also known as a subject access request, data subject access request or right of access request
- the right to ask us to change any information you think is not accurate or complete – this is called ‘right to rectification’
- the right to ask us to delete your personal information – this is called ‘right to erasure’
- the right to ask us to stop using your information – this is called ‘right to restriction of processing’
- the ‘right to object to processing’ of your information, in certain circumstances
- rights in relation to automated decision making and profiling (*The Crypt School does not take any decisions or conduct profiling by automated means*)
- the right to withdraw consent at any time (where relevant)
- the right to complain to the Information Commissioner if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it.

Contact us

If you have any questions or concerns about the way we are collecting or using your personal data, we request that you raise this with us in the first instance by contacting the Compliance Officer (foi@crypt.gloucs.sch.uk).

Alternatively, you can contact the School’s Data Protection Officer at: Gloucestershire County Council, School’s Data Protection Team, Information Management Service, Shire Hall, Westgate Street, Gloucester GL1 2TG, (tel. 01452 583619 or email schoolsdpo@gloucestershire.gov.uk).

Should you wish to, you may make a complaint to the Information Commissioner’s Office at <https://ico.org.uk/global/contact-us/contact-us-public/>

Last updated: January 2026

Annex: How Government uses your data

The workforce data that we lawfully share with the Department for Education (DfE) through data collections:

- informs the Department for Education (DfE) policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (DfE) including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

Sharing by the Department for Education (DfE)

The Department for Education (DfE) 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 for Education (DfE) will only share your personal data where it is lawful, secure and ethical to do so and 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 the Department for Education (DfE) releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of public benefit, proportionality, legal underpinning and strict information security standards.

For more information about the Department for Education's (DfE) 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 for Education (DfE) has provided information, (and for which project) please visit the following website:

<https://www.gov.uk/government/publications/dfe-external-data-shares>

How to find out what personal information the Department for Education (DfE) hold about you

Under the terms of UK GDPR, you're entitled to ask the Department for Education (DfE):

- if they are processing your personal data

- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

or

<https://www.gov.uk/government/publications/requesting-your-personal-information/requesting-your-personal-information#your-rights>

To contact the Department for Education (DfE): <https://www.gov.uk/contact-dfe>