School Staff, Governor and Volunteer PRIVACY NOTICE

General Data Protection Regulations 2018

We, at Rivers ESC, are a data controller for the purposes of the General Data Protection Regulations (GDPR).

Where the term 'staff' is used within this policy, where deemed appropriate for safeguarding and/or data protection purposes, this can also apply to other individuals working within the school.

Why do we collect and use your information?

We will only use your personal information where the law allows us to.

Under Article 6 of the General Data Protection Regulation (GDPR), we collect and use information because we are legally required to collect some information about staff, governors and volunteers and we need to process this information due to a **legal obligation** and public interest, to perform pre-employment checks and keep relevant and/or employment records. In addition, due to the safeguarding requirements of our school, we also collect information for the reason of **vital interest**: the processing is necessary to protect someone's life. Normally, we will hold data due to a contract between the school and our staff as employees.

Under Article 6 and Article 9 of GDPR, where the above lawful basis does not allow us to collect essential personal information, we will use **explicit consent** or because the processing is necessary to protect the **vital interest** of the data subject, including CCTV footage (see separate CCTV policy). Explicit consent would be sought if biometric data was ever to be collected/used by the school in the future.

How do we use your information?

We process personal data relating to those we employ to work at, or otherwise engage at our school. This is for employment purposes to assist in the running of the school (the reason for Lawful Basis) and/or to enable individuals to be paid or contacted. It could include all legal matters of employment in addition to necessary safeguarding, performance, training, sickness and grievance information. The collection of this information will benefit both national and local users by:

- improving the management of workforce data
- enabling development of a comprehensive picture of the workforce/volunteers and how they are deployed
- appropriately informing the public about our workforce/volunteers
- to help ensure effective Child Protection measures are included in our staff appointment process
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body to ensure that the school can provide an effective education (eg video conferencing, if recorded)

The data we keep on a Lawful Basis includes personal data identifiers such as contact details, National Insurance numbers, characteristics such as ethnic group, employment

contracts and remuneration details, qualifications and absence information. Some of this data is retained due to legal requirements and some as a requirement of the Single Central Record. Some key information is contained within the required School Emergency Response Plan.

After you leave us, we will keep data no longer than that required by law and/or the recommendation from County.

If you require more information about how we and/or DfE store and use your personal data please see the end of this document for further details.

Categories of information that we collect, hold and share

Any relevant information for employment purposes, including personal details (such as name and address), personal characteristics (such as ethnicity, language, nationality **if** required by the Single Central Record), information about your contract, absence, qualifications and any other specific information regarding specific need, including relevant medical information.

Collecting this information

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, the local authority or other background check agencies. We will perform online searches as part of the recruitment process, in line with guidance from Keeping Children Safe in Education (KCSIE). To comply with the General Data Protection Regulations, we will inform you if you have a choice in this.

We will also collect additional personal information throughout the period of you working for us.

Storing data

We will hold the data for as long as we are required to by law but not longer than is recommended by county. An annual sweep of the school network will be used to ensure that such data is protected and removed from general access where appropriate.

Data is backed up onsite daily. Data held is held on external databases only when necessary and such databases will have been checked for alignment to GDPR.

Who do we share your information with?

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

We may transfer your personal information outside national borders to comply with the law. If we do, you can expect a similar degree of protection to that provided by UK law, in respect of your personal information.

School Staff, Governor and Volunteer PRIVACY NOTICE

General Data Protection Regulations 2018

Why we share information

We are required to provide certain information to HMRC and Schools Pension Company to maintain staff employment within the school. We will need to release information to the Police during investigations if they make a request.

The following activities are often but not always carried out by third-party service providers:

- payroll
- pension administration
- benefits provision and administration
- IT services
- online background check during the recruitment process.
- safeguarding purposes

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, where it is needed in the public interest or for official purposes, or where we have your consent.

Department for Education

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment educational attainment.

We are required to share information with the Department for Education (DfE) under regulation 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 as amended.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers) or we may be unable to discharge our obligations which may be in the public interest or for official purposes.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

“Special categories” of particularly sensitive personal information require us to ensure higher levels of data protection. We need to have further justification for collecting, storing

and using this type of personal information. We may process special categories of personal information in the following circumstances:

- in limited circumstances, with your explicit consent.
- where we need to carry out our legal obligations and in line with our data protection policy.
- where it is needed in the public interest, such as for equal opportunities monitoring (or in relation to our occupational pension scheme), and in line with GDPR.
- where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use particularly sensitive personal information in the following ways:

- we will use information relating to leaves of absence including the reasons for the leave, which may include sickness absence or family-related leave, sabbaticals, to comply with employment and other laws.
- we will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to comply with the Equality Act 2010, to monitor and manage sickness absence and to administer benefits.
- we will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- we may use trade union membership information to pay trade union subscriptions, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use your particularly sensitive information in accordance with our written policy where processing is necessary:

- to carry out our legal obligations or exercise specific rights in the field of employment law;
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- to share information with county Governance support and Governor Hub;
- for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to

data protection and we provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In other circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of a contract of employment with us that staff agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations, provided we do so in line with GDPR.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of our recruitment, social media and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with us.

We will only collect information about convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a re-consideration.
- Where it is necessary to meet our obligations under your employment contract and ensure that appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have

notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Working from home

In the event of staff being instructed to work from home due to school closure, through management or government instruction, data required to do their job effectively may be taken home. It is preferred that this data is stored on a school device/network, however, any data taken/copied in any format should be protected adequately from other members of the household and from theft (stored safely and securely when not in use). Any data not required at home when usual school-based work resumes, must, under normal circumstances, be returned safely to the workplace within two weeks. Staff will be permitted to use personal devices to a greater degree than that permitted by standard policy during this time, in order to carry out work duties as necessary, but only whilst extraordinary working practices operate. Staff must adhere to the standard policy on the use of personal electronic devices when usual school operation resumes, or when extraordinary use is no longer required. If personal devices are used, they should be adequately protected with passwords, which should remain confidential.

Staff may be asked to provide information to county and or other school related organisations in an unusual manner during a school closure/partial closure/government/business office closure. School staff should ensure, that the method used to provide information, and the information itself, is in line with general GDPR practices to maintain compliance, but those methods can be adapted as required to suit any extraordinary working conditions.

Governors may use any school provided or self-collated, redacted or non-redacted school data, in line with their roles and responsibilities as school governors. Volunteers may use data provided to them by senior leaders and teachers, in line with their roles, as outlined by school staff. All non-employed persons must return or destroy school data if requested by senior staff and at the termination of their roles within the school. School data should not be shared outside of expected and agreed roles without express permission of the Headteacher or senior staff.

DfE data collection requirements

The following is information provided by the DfE concerning the reason it collects data about school employees, governors or volunteers:

- The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

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

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

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

The DfE 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 the DfE's 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 DfE'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

How secure is your information with third-party service providers?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?

We may share your personal information with other third parties, for example in the event of joining a Multi Academy Trust or Federation. We may also need to share your personal information with a regulator or to otherwise comply with the law.

From time to time, we may disclose your personal data in response to a request for information pursuant to the Freedom of Information Act 2000 or following a data subject access request. We may approach you for your consent but, in any event, we will only disclose your personal data if we are satisfied that it is reasonable to do so in all the circumstances. This means that we may refuse to disclose some or all of your personal data following receipt of such a request.

School Staff, Governor and Volunteer PRIVACY NOTICE

General Data Protection Regulations 2018

Data Security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties who are processing personal data on our behalf will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the school on your request.

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

How long will we use your information for?

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements. Once you are no longer an employee, worker, contractor, volunteer or governor of the school, we will retain and securely destroy your personal information in accordance with our data retention policy **or** applicable laws and regulations. Your personal information is kept in line with national requirements. We keep employment/HR and appraisal records for 7 years after staff leave the school's employment unless we are required by law to keep this information for longer. Financial records will be kept for 7 years from the end of each accounting period, or in line with national requirements.

Emails will usually be retained within school for a period of two years, unless the information contained needs to be kept longer than this (professional judgement/SLT discretion).

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current.

School Staff, Governor and Volunteer PRIVACY NOTICE

General Data Protection Regulations 2018

Please keep us informed if your personal information changes during your working/voluntary relationship with us.

Your rights in connection with personal information

In line with the GDPR policy you have the right to the following (see bullet point list below) in respect of the data held about you. However, in certain situation such as but not restricted to the safeguarding of children, this data may not be disclosed.

- **Request access** to your personal information (data subject access request). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

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 staff 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.

No fee usually required

You will not usually have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded, excessive. Alternatively, we may refuse to comply with the request in such circumstances or if we have another valid reason for doing so

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

School Staff, Governor and Volunteer PRIVACY NOTICE

General Data Protection Regulations 2018

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Inform the Headteacher or contact the Data Protection Officer (DPO) below. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

For further information

This is an additional policy which relates to staff at the school. To see our general Privacy Notice, please visit the policy section of our school website.

If you want to see a copy of information about you that we hold, please contact the school office. You can contact the Data Protection Officer at dpo@rivers.herts.sch.uk

You can contact the ICO at any time on 0303 123 1113, email https://ico.org.uk/global/contact-us/contact-us-public/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

To find out more about your rights:

- https://ico.org.uk/your-data-matters/
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To find out more about school governance in Hertfordshire:

- https://www.hertfordshire.gov.uk/about-the-council/volunteering/schools-and-youth-work/school-governor/school-governors.aspx
- hdc.governors@hertsforlearning.co.uk

School Staff, Governor and Volunteer
PRIVACY NOTICE
General Data Protection Regulations 2018

Policy Review – GDPR

This policy will be reviewed in full by the Governing Body every three years. 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.

The policy was last reviewed and agreed by Governing Body: July 2026

Name ……

Signature ……. Date …….
Headteacher

Name ……

Signature ……. Date …….
Chair of Governors

Privacy Notice Addendum: Generative AI

For use alongside the main Privacy Notices

Purpose of this addendum

This addendum supplements the existing privacy notices used by the school, academy, trust or setting. It explains how personal data will be approached when generative artificial intelligence (AI) tools are used. It does not replace the existing privacy notices and should be read alongside them.
Generative AI means technology that creates new digital content, such as text, images, audio, video or other data, in response to instructions or information provided by a user. Generative AI may operate as a standalone service or as a feature within another approved system, such as an email, document, learning or administration platform.

Who this applies to

This addendum applies where personal data about pupils or students, parents or carers, staff, volunteers, governors, trustees, committee members, visitors or other individuals is processed through an approved generative AI tool. It also covers personal or technical data collected when an individual uses an approved AI service through an organisational account.

When generative AI tools may be used

The school, academy, trust or setting will only use generative AI tools where there is a clear, necessary and proportionate reason for doing so. Examples may include supporting teaching and learning, preparing resources, assisting with administration, drafting communications, summarising information or supporting the delivery and improvement of education services.
Approval of an AI tool does not automatically approve every possible use of it. The proposed purpose, the information involved and the risks to individuals will also be considered, particularly where children, special category data, criminal offence data, safeguarding information or other sensitive information may be involved.

School Staff, Governor and Volunteer PRIVACY NOTICE

General Data Protection Regulations 2018

Personal data that may be processed

Depending on the approved tool and how it is used, personal data may include:

- information entered into a prompt or instruction;
- documents, images, audio, video or other files uploaded to, or accessed by, the tool;
- content generated by the tool and any corrections, comments or feedback added by a user;
- account details, user identifiers, usage information, interaction history and audit logs;
- technical information such as IP address, approximate location, device, operating system, browser and system information; and
- information available through approved connected services, such as email, documents, calendars, chats or other organisational content which the authorised user already has permission to access.

Legal basis and safeguards

Where generative AI is used to process personal data, the relevant data controller will identify an appropriate lawful basis under Article 6 UK GDPR. Where special category data is involved, a separate condition under Article 9 UK GDPR will also be identified. Criminal offence data will only be processed where the additional legal requirements are met.
Only the minimum personal data necessary for the approved purpose will be used. Personal, confidential or sensitive information must not be entered into an unapproved or public AI tool. Where practical, personal data will be removed, anonymised or replaced with non-identifying information before an AI tool is used.
An AI tool will only be approved to process personal data where its contractual and technical arrangements provide appropriate protection. This includes ensuring that the information is not used to train public AI models, for advertising or for unrelated purposes.

Assessment and approval

A Data Protection Impact Assessment or other proportionate risk assessment will be completed before an AI tool, or a materially different use, is introduced where personal data may be processed. It will consider necessity, the data involved, accuracy and bias, age restrictions, safeguarding, human oversight, supplier and sub-processor arrangements, security, international transfers, storage, retention and deletion.
If a high risk cannot be mitigated, the processing will not begin until appropriate further steps have been taken, including consultation with the Information Commissioner's Office where required.

How personal data will be handled

Where personal data is retained within an approved AI service, it will be held within an approved managed account or supplier environment and protected by appropriate access controls and security measures. It will be retained only for as long as necessary for the approved purpose, in accordance with the relevant retention arrangements and the terms applying to the service, and will then be securely deleted or anonymised.
Details of approved suppliers, the purposes for which they may be used and their processing arrangements will be recorded in the Supplier Compliance Log and, where appropriate, the relevant Data Protection Impact Assessment. Where an AI-generated output forms part of an education, employment, safeguarding, complaint, decision-making

or other official record, it may be retained with that record for the applicable retention period.

Human review and decision-making

AI-generated content may be incomplete, inaccurate or biased. An appropriately authorised person will review and, where necessary, correct relevant output before it is relied upon, communicated or added to an official record.
Generative AI will not be used as the sole basis for a decision which produces legal or similarly significant effects for an individual unless the use has been specifically assessed, a lawful basis and the required safeguards are in place, and the individual has been given any additional information required by law.

Individual rights

Individuals retain the data protection rights explained in the main Privacy Notices. Requests or concerns relating to personal data processed through an AI tool should be directed to the school, academy, trust or setting using the contact details provided in those notices.

Review

This addendum should be reviewed when the school, academy, trust or setting introduces or materially changes an AI tool or its use, when supplier arrangements change, or when relevant legislation or national guidance is updated.