400 YEARS OF EXCELLENCE

General Data Protection Regulation Privacy Notice (UK GDPR)

Policy approval date	**July 2026**
Policy review date	**July 2029**
Policy Lead	**Matthew Greenwood Deputy Headteacher**
Governor or SLT approval	**Governor Approval**
Governor committee responsible for policy	**Finance**

.

General Data Protection Regulations 2018

We, Richard Hale School, are a data controller for the purposes of the General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018.

The purpose of this document is to conform with your legal right to be informed about how the school collects, stores, uses or shares any information we hold about you or your child. For the purpose of this document, 'pupil information' includes any relevant details about parents, carers or persons responsible for the child.

Why do we collect and use pupil information?
Under Article 6 of the UK GDPR (abbreviated to GDPR in this document), we collect and use information because we are legally required to collect some information about pupils and staff and we need to process this information due to our **legal obligation** (6,c) to provide an education to our pupils. This includes sharing information with exam boards, other schools and the Department of Education (DfE) where necessary. Our operation necessitates the use of **contracts** (6,b) including home-school contracts and contracts with staff and suppliers. In addition, due to our safeguarding responsibilities, we also collect information for the reason of **vital interest** (6,d) where the processing is necessary to protect someone's life. CCTV footage is recorded and a separate CCTV policy exists. Occasionally we collect and process data as a requirement for a **public task** (6,e), which could include collecting evidence of our duty to educate children, in the form of a learning or communication platform, or the capture of images/video/sound at school events, such as sports day and concerts/productions. We may also record telephone calls for safeguarding, training, or monitoring purposes. Where recording is in operation, callers will be informed at the start of the call.

Under Article 6 and Article 9 of GDPR, where the above lawful bases do not allow us to collect essential personal information, we will use **consent** (6,a) where the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

We may receive information about them from their previous school, the Department for Education (DfE) and Hertfordshire County Council. We hold this personal data to:

- support the learning in our school
- monitor and report on pupil progress
- provide appropriate pastoral care
- assess the quality of our services
- keep our pupils and staff safe
- comply with the law regarding data sharing

The categories of information that we collect, hold and share include:
Personal details (such as name, Unique Pupil Number and address), national curriculum assessment results, attendance information (such as sessions attended, number of absences and absence reasons), any exclusion information, where they go after they leave us, personal characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility), any special educational needs they may have as well as relevant medical information. Sensitive personal information may also be processed for safeguarding purposes (on the Legal Basis of **Vital Interest**) at any time. Explicit consent would be sought if biometric

data was ever to be collected/used by the school in the future.

Collecting pupil information
We collect pupil information by using registration forms, data collection forms (which may be used annually) or file transfer from previous schools.

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 General Data Protection Regulations, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Use of AI Technologies
The school may use AI-assisted technologies for administrative and educational purposes. For details on how AI is applied and safeguards in place, please see our AI policy and Addendum in the Appendix below.

Storing data
An annual sweep of the school network will be used to ensure that data is removed from general access where appropriate. We shred or destroy redundant data onsite.

We may hold data on USB memory devices if adequately protected, although their use is discouraged.

Photographs, videos and sound media will be captured by the school using school equipment and in line with any consent granted.

Data is backed up regularly (details can be obtained from the School Office). Arbor and MyConcern are online services, backed up by the service providers (details are held within our Supplier Compliance Log). We maintain a supplier compliance log to ensure that Data Processors (our suppliers) are compliant and effectively safeguard your data.

The school has robust processes in place to minimise the risk of data breaches. In the unlikely event of a Data Breach, the school has an internal Data Breach Procedure and documentation which would be followed. These documents are overseen by the school's Data Protection Officer (DPO). In the event of a data breach, we would act in accordance with the General Data Protection Regulations 2018.

Data Retention
Personal data is retained in accordance with the Department for Education (DfE) Data Retention Schedule 2025. The school cannot agree to delete pupil data during a child's time in education, as much of this information is required to deliver statutory and safeguarding responsibilities.
Once a pupil leaves a school within the school, records are transferred securely to their next school or education provider, or to the relevant local authority where required.

For pupils with special educational needs (SEN), educational records are retained until the academic year of their 25th birthday, in line with statutory guidance. For all other pupils,

records are normally removed from general access two years after they leave the school, once educational and safeguarding files have been transferred appropriately.
A formal annual review of school records is carried out to ensure that data is archived or securely deleted when no longer required.

Certain categories of information are kept for longer in line with legal or operational requirements – for example:

- Financial and accounting information and Data Breach Logs are retained for seven years
- Emails are retained for up to two years unless there is a lawful or operational reason to keep them longer, as determined by senior leadership

Where a major incident occurs – such as a safeguarding, medical or critical incident involving external agencies – full records may need to be retained until the youngest person involved reaches the age of 25, or longer if required by law or regulation.

Who do we share information with?
We will not give information about you or your child to anyone without your consent unless the law and our policies allow us to.

Where our school is involved in collaborative delivery with other schools and learning providers, pupil information may also be shared to aid the preparation of learning plans and the use of data to achieve the objectives identified above or with schools that the pupil attends after leaving us. We need to share information, on occasion with (but not limited to) Virtual Schools, Education Psychologist, transfer schools, Social Services Assessment Team, Children's Services, school governors/trustees, local authority support services including the NHS, police and courts as necessary, and other health related assessment teams including disability allowance. We are required, by law, to share some information with the Department for Education (DfE). This information will, in turn, then be made available for the use by the Local Authority. Additionally, the curriculum may require the use of third party web-based learning platforms, if GDPR compliant. We may share information with our Parents' Association if we have your consent.

Why we share information
We are required to share information about our pupils with the (DfE) under regulation 4 and 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Whilst we share information as an ongoing school management requirement, which would include non-standard operational activity such as promoting the school and complaints/legal proceedings as required, we do not share information about our pupils with anyone without your consent unless the law and our policies allow us to do so.

Safeguarding
GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place

a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place.

Data collection requirements
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.

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- our local authority at http://www.hertsdirect.org/services/edlearn/privsch/ or
- the DfE website at https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

How Government uses your data
The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

The National Pupil Database (NPD)
Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils 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.

To find out more about the NPD, go to:
https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, parents, carers and data subjects over the age of 13 have the right to request access to information that we hold about them or their child.

Parents/carers can request information about their child without consent from the data subject, until the child reaches 17 years of age. To make a request for your personal information, or be given access to your child's educational record, contact the school office or email the Data Protection Officer (see 'Contact' below). Please be aware that in certain situations such as, but not restricted to safeguarding, this data may not be disclosed. A form may be provided to help with this process.

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 purposes of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed
- claim compensation for damages caused by a breach of the Data Protection regulations
- withdraw any consent that you have provided**

To find out more about your rights, visit https://ico.org.uk/your-data-matters/

**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.

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 or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Cookies

Our website uses Cookies to track visits to our website but we do not use it to identify you or for marketing purposes. You do not have to use our website as the information can be provided to you by the school office at your request.

Concerns

We understand that there are penalties for inadequately protecting your data or for non-compliance with the GDPR. If you have a concern about the way we are collecting or using your personal data, you can raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/, on 0303 123 1113 or via email by visiting https://ico.org.uk/global/contact-us/email/

Contact

If you wish to access personal data held about you or your child, please contact:

- Richard Hale School, Hale Road, Hertford SG13 8EN. Tel: 01992 583441
- dpo@richardhale.herts.sch.uk

Additional Contact Details

- LA's Data Protection Office: Information Governance Unit, Room C1, County Hall, Pegs Lane, Hertford, SG13 8DQ, email: dataprotectionhertscc.gov.uk
- QCA's Data Protection Officer: 83 Piccadilly, London, W1J 8QA
- DfE's Data Protection Office Caxton House, Tothill St, London, SW1H 9NA
- Ofsted Data Protection Office: Alexandra House, 33 Kingsway, London, WC2B 6SE

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.

APPENDIX – A : Addendum: Generative AI

Purpose of this addendum

This addendum supplements the existing privacy notices used by the school. 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.

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 will be reviewed when the school introduces or materially changes an AI tool or its use, when supplier arrangements change, or when relevant legislation or national guidance is updated.

APPENDIX B: Addendum: Biometric Data

Purpose of this addendum

This addendum supplements the existing privacy notices used by the school. It explains how biometric data will be used. It does not replace the existing privacy notices and should be read alongside them.

Biometric data means personal data resulting from specific technical processing relating to a person's physical, physiological or behavioural characteristics. Examples include fingerprints, facial recognition data, iris or retina scans, palm vein data, voice recognition data and similar identifiers. Where biometric data is used for the purpose of uniquely identifying a person, it is special category data.

Who this applies to

This addendum applies where biometric data is processed about pupils or students, parents or carers, staff, volunteers, governors, trustees, committee members, visitors or other individuals who may use or be affected by a biometric recognition system operated by, or on behalf of, the school, academy, trust or setting.

When biometric systems may be used

The school, academy, trust or setting will only use biometric systems where there is a clear, necessary and proportionate reason for doing so. Examples may include cashless catering, library access, access control, attendance systems or similar education management purposes. Before introducing or materially changing any biometric system, the relevant data controller will consider whether a less intrusive alternative can achieve the same purpose.

Legal basis and safeguards

Before using biometric data for identification, the relevant data controller will identify an appropriate lawful basis under Article 6 UK GDPR and a separate condition for processing special category data under Article 9 UK GDPR. In most education biometric recognition contexts, explicit consent is likely to be required.

For pupils and students under 18, the school, academy, trust or setting will also comply with the Protection of Freedoms Act 2012. This means parents or carers will be notified before the child's biometric information is processed, the required written parental consent will be

obtained, any written parental objection or withdrawal of consent will be respected, and a pupil's or student's own objection or refusal will also be respected.

Data Protection Impact Assessment

A Data Protection Impact Assessment will be completed before introducing, or materially changing, a biometric recognition system. The assessment will consider the purpose of the system, whether the processing is necessary and proportionate, the risks to individuals, the supplier arrangements, security measures, retention arrangements and the availability of reasonable alternatives.

If a Data Protection Impact Assessment identifies a high risk that cannot be mitigated, the processing will not begin until the appropriate further steps have been taken, including consultation with the Information Commissioner's Office where required.

Consent, refusal and alternatives

- Where consent is used, it must be freely given, specific, informed and capable of being withdrawn.
- For pupils and students under 18, the written consent of at least one parent or carer with parental responsibility is required, unless a statutory exception applies, and no parent or carer has objected or withdrawn consent.
- A pupil or student may refuse or object to the use of their biometric data. Their objection does not need to be in writing and will override parental consent.
- A reasonable non-biometric alternative will be provided so that individuals are not disadvantaged because they do not use the biometric system.
- Where consent is withdrawn, or the individual ceases to use the system, the relevant biometric data will be securely deleted unless there is a lawful reason to retain it.

How biometric data will be handled

Where biometric data is used, separate information will be provided explaining the specific system being used, the type of biometric data collected, the purpose of the processing, who will have access to the data, whether a processor or supplier is involved, how the information will be secured, how long it will be retained and how it will be deleted.

Biometric data will only be used for the purpose explained at the point consent is sought or information is provided. It will not be used for unrelated purposes without further assessment and, where required, fresh consent and updated privacy information.

Live facial recognition

Live facial recognition will not be used in school. Live facial recognition is different from a controlled biometric recognition system and involves the real-time and potentially indiscriminate capture of biometric data from people passing within range of a camera. Current DfE guidance states that live facial recognition is not appropriate in school and college settings.

Review

This addendum will be reviewed when the school, introduces or changes any biometric system, when supplier arrangements change, or when relevant legislation or national guidance is updated.