

Ribblesdale School

Privacy Notice (How we use pupil information)

Ribblesdale School is the Data Controller for the use of personal data in this privacy notice.

We collect and use information about pupils to support their learning, keep them safe, and promote their health and wellbeing.

The categories of pupil information that we collect, hold and share include:

- Personal information and contacts (such as name, unique pupil number, address, phone numbers, email addresses, pupil premium)
- Family details (parents/carers names, addresses, phone numbers, email addresses)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility, looked after children, post looked after children, service children, school history, GP surgery)
- Attendance information (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment information
- Medical conditions and administration (such as doctors information, child health, allergies, medication and dietary requirements) plus agency involvement if relevant i.e. therapist, paediatrician
- Special Educational Needs and Disability (including the needs and ranking)
- Behaviour and exclusions (such as exclusions and any relevant alternative provision put in place)
- Information relating to catering and free school meals
- Post-16 destinations
- CCTV images captured in school
- Photographs/ videos
- Biometric data (fingerprint recognition system for cashless catering)
- Safeguarding information (such as court orders and professional involvement etc)

Why we collect and use this information

The personal data collected is essential for the school to fulfil their official functions and meet legal requirements.

We collect and use pupil information, for the following purposes:

- to support pupil learning

- to monitor and report on pupil progress
- to provide pastoral care
- to assess the quality of our services
- to safeguard pupils
- to keep children safe (food allergies or emergency contact details)
- to meet statutory duties (including Department for Education data collections)
- to comply with legal obligations
- to provide additional activities for pupils, such as school trips and extra-curricular activities
- to assist with the administration and communication systems – for example, cashless catering
- to provide wraparound care in the out of school club
- to administer admissions

We may also share information without consent where it is necessary to protect a pupil or others from harm.

The lawful basis on which we use this information

We will only use your information when the law allows us to. Under the UK General Data Protection Regulation (UK GDPR), the lawful basis/bases we rely on for processing pupil information are:

Article 6 (1) GDPR

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
 - (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes (for example, some photographs/video images);
 - (c) processing is necessary for compliance with a legal obligation to which the controller is subject (for example – to meet our responsibilities under law i.e. Keeping Children Safe in Education);
 - (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person (for example, passing on information about a pupil's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that pupil or another individual);
 - (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (for example, to fulfill our official duties as a school);

For 'special category' data under Article 9, we only collect and use it when we have both a lawful basis, as set out above, and the conditions we may rely on for processing special category data are:

Article 9 GDPR (special category data)

- (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
- (2) Paragraph 1 shall not apply if one of the following applies:

- (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject (for example, fingerprints)
- (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The Education Act 1996 – Section 537A – states that we provide individual pupil information as the relevant body such as the Department for Education.

Children's Act 1989 – Section 83 – places a duty on the Secretary of State or others to conduct research.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Biometric Information

The school operates an automated (i.e. electronically operated) biometric fingerprint recognition system for purchases from the school catering services. All data collected will be processed in accordance with the Data Protection Act 2018 and the Protection of Freedoms Act 2012. The written consent of at least one parent/carer will be obtained before biometric data is taken and used. If one parent objects in writing, then the school will not take or use a child's biometric data.

Collecting pupil information

We collect pupil information via registration forms/admissions process at the start of school year, Common Transfer File from your previous school, secure file transfer from previous school or Child Protection plans. We occasionally collect information face to face, via telephone calls and emails.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

Storing pupil data

We retain pupil data in line with the Information and Records Management Society (IRMS) Schools Toolkit for Data Protection.

International data transfers

Some of the systems we use (such as cloud-based services) may store or process personal data outside of the United Kingdom. Where this occurs, we ensure that appropriate safeguards are in place in accordance with UK data protection law.

Who we share pupil information with

We routinely share pupil information with:

- the local authority (LCC – to share certain information, such as safeguarding concerns and information about exclusions. Some of this data is shared via Wonde (Wonde Privacy Notice available on request.))
- the pupil's family and representatives
- the Department for Education (DfE)
- NHS/school nurse/health care professionals including IntraHealth/ HCRG (school nursing and immunisation services)
- youth support services including counselling services
- the appointed school photographer
- school staff and governing body
- catering supplier
- IT and cloud storage providers
- vocational course providers
- extra-curricular/enrichment activity providers
- after-school clubs
- law enforcement officials such as police, courts
- examining bodies
- professional advisers and consultants
- educational institutions that pupils attend after leaving us
- SIMS
- Ofsted
- disclosure connected with SEND support – e.g. professional providing therapy or educational interventions, such as speech and language therapy
- post-16 education providers such as colleges and sixth form providers
- suppliers and service providers, to enable them to provide the service we have contracted them for including but not limited to:
 - Education Digital Services – Lancashire CC (School management systems including SIMS)
 - Tucasi (Scopay)
 - CPOMS (Child Protection, safeguarding and behaviour system)
 - InVentry (entry and exit system)
 - Freedom Tech (121 device supplier)

- School Cloud (Parents' Evening software)
- Synergy (whole school communication platform)
- Every (asset management)
- School Work Space (Exams Assist)
- Microsoft Office 365 – including Nurture
- Applica (online management of admissions/data collection)
- Wonde – secure data transfer between the school's database and DfE/ LCC/ Holiday Activities/FFT Aspire/Accessit Library System/GL Assessment/ Sparx Learning/ Tassomai/ Welfare Call Group/ LCC
- Classroom software resources including Doodle, Class Charts, Tassomai, Unifrog, SeeSaw
- The Nursery Milk Scheme
- Blackout Technologies 'Blackout App' – device monitoring system

We only share the minimum amount of information necessary.

The school shares class list information with providers in connection with the following public health screening programmes:

National Child Measurement Programme (NCMP)

The lawful basis for processing personal data is:

Art. 6 (1) (e) GDPR: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The personal data processed in respect of the public health screening programmes includes personal data revealing ethnic origin which is classified as special category personal data under Art. 9 GDPR which merit special protection and consequently a further condition for processing is required.

The additional lawful basis for processing special category personal data (specifically ethnic origin) is:

Art 9 (2) (h) GDPR: Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

Dental Screening Survey & Vision Screening Programmes

The lawful basis for sharing personal data is:

Art. 6 (1) (e) GDPR: Processing is necessary for the performance of a task carried out in the public interest.

The additional lawful basis for processing special category personal data is:

Art 9 (2) (h) GDPR: Processing is necessary for the provision of health or social care.

The legitimate interest is to provide public health services and improve health and wellbeing outcomes for children and young people, which falls outside the task of schools as public authorities to provide education to children and young people.

Processing is necessary as only schools hold up to date class list/address data to facilitate:

- Any necessary follow-up arrangements, in response to identified need or to promote health and wellbeing, by a health professionals. Contact is arranged with the child/ young person or with parents/ carers.

- Any appointments being sent to the parent/carer of a child who requires further assessment of their optical health needs – or to arrange follow-up

School Nursing: Collection of Health Assessments/Questionnaires at Reception, Year 6 and Year 9

The Lancashire Healthy Young People and Families Service (HCRG Care Group) are a provider of school nursing services in Lancashire. The school shares class list information (such as name, date of birth and school details) for the purposes of the collection of health assessments (Reception, Year 6 and Year 9) with school nursing services.

The school can share this information with school nursing services using under the following lawful bases:

Article 6(1)(e) UK GDPR – processing is necessary for the performance of a task carried out in the public interest

Article 9(2)(h) UK GDPR – processing is necessary for the provision of health or social care

These lawful bases allow the school and health services to work together to safeguard and promote the wellbeing of pupils.

School Nursing services offering support to address individual health needs. School Nurses and their employing organisation will have access to children's individual information, in order for them to identify and offer further support to children or young people who require their services. School Nurses adhere to national standards of confidentiality unless they have cause for concern around best interest/ safety issues. The School Nurses will keep a record of the health assessment/ questionnaire within the Child Health Record.

The information collected from questionnaires will also be used to form a summary report for the school. This is anonymised information that will support schools to understand the health needs of their pupils and allow them to target resources appropriately. The School Nurses may provide advice to school in response to these anonymised reports to help understand and respond to the health needs of the school.

The Local Authority being Lancashire County Council will also use this information at an anonymised level in order to understand and address the population health needs of children and young people in areas of Lancashire and make appropriate plans and actions.

IntraHealth – MAVIS (Manage Vaccinations in Schools)

The school works with NHS-commissioned vaccination providers and uses the MAVIS (Manage Vaccinations in Schools) platform to support the safe and efficient delivery of school-based immunisation programmes. The immunisation team will use MAVIS, a secure digital system to send consent forms directly to parents. The type of information shared may include:

- Class lists
- Pupil name, date of birth, gender, address and school details
- Parent/carer contact information
- NHS number (where available)

Information is shared with:

- NHS vaccination providers (e.g. School Age Immunisation Service)
- Relevant healthcare professionals involved in delivering vaccinations

Lawful basis for sharing:

UK GDPR Article 6(1)(e): Public task

UK GDPR Article 9(2)(h): Provision of health or social care

Consent for vaccinations is obtained directly from parents/carers by the NHS provider via the MAVIS system.

All information is handled through secure systems with restricted access. Only authorised school staff and healthcare professionals can access the data. Data is retained in accordance with NHS and local authority retention schedules. IntraHealth acts as an independent Data Controller for the information they receive and processes data in line with their own privacy notice.

Blackout App – Blackout Technologies

The School uses the Blackout App which is a device management solution for schools to restrict functionality on personal mobile devices during the school day only.

Information shared includes:

- Pupil name
- School email address
- Year group
- Device type and operating system eg iOS 16
- Basic device status information during restricted hours (e.g. whether Blackout is active and correctly configured)

No personal content is accessed. There is no location tracking and no browsing history is collected.

The lawful basis for processing is:

UK GDPR Article 6(1)(e): Public Task

The Blackout App operates during the school day only, once the school schedule ends, the app gives full control of the device back to the pupil.

We only share the minimum amount of information necessary. The data is shared with Blackout Technologies (who acts as a data processor on behalf of the school and processes data in line with UK data protection legislation) and authorised school staff.

Data is only retained for the duration of the school's use of the service. When a pupil leaves school, or when the contract ends, their account and associated device data are deleted.

Why we share pupil information

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

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE).

We may share information without consent where it is necessary to protect a pupil or other individuals from harm or to fulfil our safeguarding responsibilities.

We only share the minimum amount of personal information necessary for the purpose.

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13–19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information we share is limited to the pupil's name, address and date of birth; however, where a parent or carer has provided their consent, other relevant information will be shared – this right to consent is transferred to pupils once they reach 16 years old.

Department for Education (DfE)

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by the Department for Education (DfE) under a combination of software and hardware controls, which meet the current [government security policy framework](#).

For more information, please see 'How Government uses your data' section.

How the government uses your data

The pupil data that we lawfully share with the Department for Education (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)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (DfE) (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>

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 (DfE) 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 for Education (DfE).

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>

Sharing by the Department for Education (DfE)

The law allows the Department for Education (DfE) to share pupils' personal data with certain third parties, including:

- schools and local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the Department for Education's (DfE) NPD data sharing process, please visit:

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

Organisations fighting or identifying crime may use their legal powers to contact the Department for Education (DfE) to request access to individual level information relevant to detecting that crime.

For information about which organisations the Department for Education (DfE) has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police 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) holds about you

Under the terms of the [Data Protection Act 2018](#), you are 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>

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

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Anne-Marie Horrocks, Headteacher, by email to enquiries@ribblesdale.org

Depending on the lawful basis above, you also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- object to processing of personal data that is likely to cause, or is causing, damage or distress
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed where there is no compelling reason for its continued processing; and
- a right to seek redress, either through the ICO, or through the courts.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

For further information on how to request access to personal information held centrally by the Department for Education (DfE), please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting Anne-Marie Horrocks, Headteacher, by email to enquiries@ribblesdale.org

Automated Decision-Making

The school does not make decisions about pupils based solely on automated processing or profiling.

Last updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in June 2026.

Contact

If you would like to discuss anything in this privacy notice, please contact:

Mrs Anne-Marie Horrocks, Headteacher,
Mrs Susan Cowking, Business Manager, or
Mrs Sarah Wilkinson, Data Protection Officer
(enquiries@ribblesdale.org)

Version number	Valid from	Valid to	Comments
1	May 2023	May 2024	Updated
2	May 2024	November 2024	Updated
3	November 2024	January 2025	Updated
4	January 2025	February 2025	Updated
5	February 2025	June 2025	Updated
6	June 2025	Sept 2026	Updated
7	September 2026		