Reviewed by: JMS
Date: Trinity. 2026
Next Review: Trinity 2027

RISHWORTH SCHOOL

DATA PROTECTION AND PRIVACY NOTICE (GDPR COMPLIANT).

Includes Appendix A: Subject Access Request (SAR) Procedure

Distribution: School Website, Staff Policy Library

This Privacy Notice is intended to be read alongside other School policies and procedures, and the School will ensure that its approach to data protection reflects its wider commitment to safeguarding, pastoral care and good governance.

1. WHO WE ARE

Rishworth School is the Data Controller responsible for personal data processed in connection with its activities.

Address:
Rishworth School
Oldham Road
Rishworth
West Yorkshire, HX6 4QA

Company Number: 05855479
Charity Number: 1115562

2. DATA PROTECTION CONTACT

The School has appointed a Data Protection Officer (DPO) to oversee compliance.

In practice, responsibility for day-to-day data handling sits with senior leaders, including the Head, Bursar and IT Engineer, who work together to ensure that personal data is handled appropriately across the School.

The DPO is Chantel Billson, email: cbillson@rishworth-school.co.uk

The DPO handles:

- Data protection queries
- Subject access requests
- Complaints and concerns

3. SCOPE OF THIS PRIVACY NOTICE

This Privacy Notice explains how the School collects, uses, stores, and shares personal data relating to:

- Students (current, past, prospective)
- Parents / Guardians
- Staff (current, past, prospective)
- Alumni and donors
- Governors and volunteers

It applies alongside other policies including, but not limited to, safeguarding and child protection, IT, CCTV, retention, and staff policies.

4. DATA PROTECTION PRINCIPLES

The School processes personal data in accordance with UK GDPR principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

5. LAWFUL BASIS FOR PROCESSING

The School relies on the following lawful bases under UK GDPR:

Article 6 (General Data)

- Contract – provision of education and employment
- Legal obligation – safeguarding, HMRC, DfE, regulatory requirements
- Legitimate interests – school operations, alumni relations, security
- Consent – limited uses (e.g. biometrics, some images, marketing)

Article 9 (Special Category Data)
Where sensitive data is processed, the School relies on:

- Substantial public interest (e.g. safeguarding, equality monitoring)
- Vital interests (emergencies)
- Legal obligations (employment/safeguarding)
- Explicit consent (where required)

6. WHY WE PROCESS PERSONAL DATA

In carrying out its duties as an independent school, the School necessarily processes personal data as part of its day-to-day operations and to support the education and wellbeing of its pupils.

In order to carry out its ordinary duties to all members of the School community the School needs to process a wide range of personal data about as part of its daily operation:

- Deliver education and pastoral care
- Safeguard students and staff
- Manage admissions and recruitment

- Administer employment and payroll
- Monitor progress and academic performance
- Meet legal and regulatory obligations
- Maintain school operations and security (including CCTV)
- Communicate with the school community
- Support alumni engagement and fundraising

These purposes reflect lawful educational and safeguarding duties

7. TYPES OF DATA PROCESSED

The School may process:

- Contact details
- Academic and assessment records
- Behaviour and safeguarding records
- Health and medical information
- Special educational needs data
- Financial and billing information
- Employment records
- Identity and immigration information
- Images, CCTV footage, and biometric data (where applicable)

8. HOW THE SCHOOL COLLECTS DATA

Personal data is collected from:

- Parents and students directly
- Staff members
- Previous schools or professionals
- Public authorities (e.g. local authority)
- Public sources where appropriate

Provision of Data
In some cases, individuals are required to provide personal data to enable the School to fulfil its contractual or legal obligations. Failure to provide such information may mean the School is unable to fulfil its responsibilities.

9. DATA SHARING

Personal data is shared only when necessary, including with:

- Examination boards
- Regulatory authorities (DfE, ISI, ICO, Charity Commission)
- Local authorities and safeguarding agencies
- Professional advisers (legal, HR, insurers)
- Contractors and service providers (under contract)

All third-party processors are subject to data processing agreements ensuring security and compliance. In most cases, information will be shared on a strictly need-to-know basis and only where it is necessary and proportionate to do so.

10. INTERNATIONAL DATA TRANSFER

Where data is transferred outside the UK, the School ensures safeguards such as:

- Adequacy regulations
- Standard contractual clauses
- Approved certification mechanisms

11. SAFEGUARDING DATA

The School recognises that safeguarding responsibilities may, at times, require information to be shared without consent where this is necessary to protect a child or other individuals.

The School processes safeguarding information in line with:

- Keeping Children Safe in Education (KCSIE)
- Legal safeguarding obligations

This may include:

- Recording concerns (including low-level concerns)
- Sharing information with safeguarding authorities
- Transferring files to new schools

Safeguarding processing is carried out under legal obligation and substantial public interest.

12. DATA RETENTION

The School retains data in accordance with its Retention Schedule, based on ICO and sector guidance.

Typical retention includes:

- Student records: variable depending on type
- Safeguarding records: until at least age 25
- Staff records: typically, 6–7 years post-employment

Data is only retained as long as necessary for lawful purposes.

In practice, different types of records are kept for different periods, reflecting both legal requirements and the operational needs of the School.

13. DATA SECURITY

The School implements appropriate technical and organisational measures, including:

- Access controls (need-to-know basis)
- Secure IT systems
- Staff training
- Encryption and secure storage
- Policies governing IT and device use

All staff receive regular data protection training

14. DATA BREACHES

The School maintains procedures to:

- Detect and investigate breaches
- Notify the ICO within 72 hours (where required)
- Inform affected individuals where there is high risk

15. CHILDREN'S DATA AND TRANSPARENCY

The School recognises that children require additional protection.

- Age-appropriate explanations are provided
- Data processing prioritises the best interests of the child
- Parents are engaged appropriately, subject to legal and safeguarding considerations

16. YOUR RIGHTS

Individuals have rights under UK GDPR, including:

- Access to personal data
- Correction of inaccurate data
- Erasure (in certain circumstances)
- Restriction of processing
- Data portability
- Objection to processing

Requests are normally handled within **one month**.

These rights are **not absolute** and may be limited where:

- Safeguarding concerns apply
- Legal obligations prevent disclosure
- Third-party confidentiality applies

The School will always seek to respond to requests promptly and helpfully, while balancing its legal obligations and the rights of others.

17. PARENT AND STUDENT REQUESTS

- Data belongs to the individual (student)
- Parents may act on behalf of younger children
- Older students' rights will be respected based on maturity
- Requests are assessed on a case-by-case basis

18. CONSENT

Where the School relies on consent:

- It will be freely given and withdrawable
- Withdrawal will not affect prior lawful processing

Consent is typically used for:

- Biometrics
- Certain image use
- Optional communications

19. AUTOMATED DECISION MAKING

The School does not carry out automated decision-making or profiling with legal or significant effects.

20. ACCOUNTABILITY AND GOVERNANCE

- The School maintains records of processing activities
- Data Protection Impact Assessments are conducted where required
- The Governing Body oversees compliance and risk

The School is committed to handling personal data responsibly and transparently, and to maintaining the trust of its community.

21. KEEPING IN TOUCH

The School may contact parents and alumni regarding:

- School updates
- Events and activities
- Fundraising

Individuals may opt out at any time.

22. COMPLAINTS

If you have concerns:

1. Contact the School or DPO
2. Use the School complaints procedure

You have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK supervisory authority for data protection matters: www.ico.org.uk

- Website: www.ico.org.uk

APPENDIX A

SUBJECT ACCESS REQUEST (SAR) PROCEDURE

1. PURPOSE

This procedure sets out how Rishworth School responds to requests from individuals seeking access to their personal data under UK GDPR (Subject Access Requests – SARs).

The School is committed to handling all requests:

- Lawfully
- Promptly
- Transparently
- In a way that protects safeguarding and confidentiality

2. WHAT IS A SUBJECT ACCESS REQUEST?

A Subject Access Request is a request made by an individual to:

- Obtain confirmation that their personal data is being processed
- Access a copy of that data
- Receive information about how the data is used

SARs can be made in writing to the school (via email or letter)

3. WHO CAN MAKE A REQUEST

Requests may be made by:

- Staff (current or former)
- Parents / guardians
- Students
- Alumni
- Third parties acting on behalf of an individual (with authority)

Children and Requests

- Personal data belongs to the child
- Parents may make requests on behalf of younger children
- Older students can make their own requests if deemed sufficiently mature
- The School will assess:
    - The child's understanding
    - Best interests
    - Safeguarding considerations

4. HOW TO SUBMIT A REQUEST

Requests should be directed to:

Data Protection Officer (DPO)
Email: cbillson@rishworth-school.co.uk

However, staff must recognise that:

- Any communication requesting personal data **may constitute a SAR**
- Staff must immediately pass such requests to the DPO

5. IDENTITY VERIFICATION

Before processing a request, the School will verify identity.

The School may request:

- Photographic ID
- Proof of address
- Evidence of parental responsibility
- Written authority for third-party requests

The response timeframe begins once identity is confirmed.

6. TIMESCALES

The School will respond:

- Within one calendar month of receiving a valid request
- This may be extended by up to two further months if:
    - The request is complex, or
    - Multiple requests are made

The requester will be informed if an extension is required.

Where clarification of scope of the request is required the timescale will start from the receipt of this clarification.

7. FEES

- SARs are normally free of charge
- A reasonable fee may be charged where:
    - Requests are manifestly unfounded or excessive
    - Repeated copies are requested

8. PROCESS FOR HANDLING REQUESTS

Step 1 – Acknowledge

- Confirm receipt
- Clarify scope if necessary

Step 2 – Clarify Scope (if needed)

- Narrow large or unclear requests
- Encourage targeted requests

Step 3 – Search for Data

The School will search relevant systems, including:

- Student records
- Emails
- Safeguarding systems
- HR records
- IT systems

Searches will be proportionate and reasonable.

Step 4 – Review and Redaction

Before disclosure, the School will:

- Remove third-party personal data unless consent is obtained or it is reasonable to disclose
- Consider safeguarding risks
- Remove legally privileged information
- Apply relevant exemptions (see Section 9)

Step 5 – Prepare Response

The School will provide:

- A copy of personal data
- Explanation of:
    - Purpose of processing
    - Categories of data
    - Recipients of data
    - Retention periods
    - Rights of the individual

Step 6 – Provide Securely

Data will be shared:

- Electronically (secure format) or
- By secure post

9. EXEMPTIONS AND LIMITATIONS

The School may withhold or redact information where permitted by law, including:

Common exemptions in schools:

- Safeguarding concerns
- Information identifying another individual
- Confidential references
- Legal professional privilege
- Examination scripts (though marks may be shared later)

The School will assess each case individually.

10. SAFEGUARDING CONSIDERATIONS

Safeguarding takes priority.

The School may refuse or limit disclosure if it:

- Could put a child or individual at risk
- Would compromise a safeguarding investigation
- Conflicts with statutory safeguarding duties

Decisions will involve the Designated Safeguarding Lead (DSL) where appropriate.

11. REQUESTS FROM OR ABOUT STUDENTS

- Older students may control access to their data
- Parental requests may be refused if:
    - The student is competent and objects
    - Disclosure is not in the child's best interests

All requests are considered on a case-by-case basis.

12. REFUSING A REQUEST

The School may refuse a request where it is:

- Manifestly unfounded
- Excessive
- Repetitive

The School will provide:

- Reasons for refusal
- Information about the right to complain

13. RECORD KEEPING

The School will keep records of:

- Requests received
- Actions taken
- Decisions made
- Reasons for exemptions or refusals

This supports accountability and compliance.

14. COMPLAINTS

If a requester is dissatisfied, they may:

1. Complain to the School (via DPO or complaints process)
2. Escalate to the **Information Commissioner's Office (ICO)**
    - www.ico.org.uk

15. STAFF RESPONSIBILITIES

All staff must:

- Recognise potential SARs
- Forward requests immediately to the DPO

- Not delete or alter records once a request is received
- Maintain confidentiality at all times

Failure to follow this procedure may result in disciplinary action.