

Privacy Notice – Staff, Volunteers and Contractors

More Than Ed | Independent School

Date: July 2026

Review Date: July 2027

Responsible Person: Jonathan Mundin

Document control

Item	Detail
Document title	Privacy Notice – Staff, Volunteers and Contractors
Version date	July 2026
Review date	July 2027
Owner	Data Protection Lead
Data Protection Lead	Jonathan Mundin
Supersedes	January 2026 version
Published	School website and available from the school office

Contents

1. Introduction	3
2. Who we are.....	3
3. What personal data we collect.....	3
4. Why we use this data and our lawful basis	4
5. How we collect your data	6
6. Who we share your data with	6
7. Transfers outside the United Kingdom	7
8. How long we keep your data	7
9. Data security.....	8
10. Your rights.....	8
11. Making a subject access request	9
12. Automated decision-making and profiling	9
13. Data protection complaints.....	9
14. Social media and online presence.....	10
15. Changes to this notice.....	10
16. Contact and complaints to the regulator	10
17. Related policies.....	10
18. Legislation and guidance.....	11

1. Introduction

More Than Ed Independent School is committed to protecting the privacy of its staff, volunteers and contractors. This privacy notice explains how we collect, use, store and share your personal data throughout your employment or engagement with the school.

It is issued in accordance with the UK General Data Protection Regulation (UK GDPR), as amended by the Data (Use and Access) Act 2025, and the Data Protection Act 2018.

This notice applies to all current and former employees, volunteers, agency and casual workers, contractors and consultants. It supplements your contract of employment or engagement and should be read alongside our Data Protection Policy. It does not form part of any contract, and we may update it from time to time.

2. Who we are

More Than Ed Independent School is the data controller for the personal data we process about our workforce. We are an independent SEMH day school providing specialist 1:1 education for students aged 7 to 16, all of whom have an Education, Health and Care Plan.

Our Data Protection Lead is Jonathan Mudin, who can be contacted at Jonathan.Mudin@morethaned.co.uk or by writing to More Than Ed Independent School, Cherry Tree Court, Woodfield Park, Balby, Doncaster, DN4 8QN.

3. What personal data we collect

3.1 Recruitment data

During the recruitment process we collect your name, address and contact details, qualifications, employment history, references, right to work documentation, and any information you disclose on your application form or at interview.

As part of our safer recruitment duties under Keeping Children Safe in Education (KCSIE) and the Education (Independent School Standards) Regulations 2014, we also process enhanced DBS certificate information, children's barred list checks, prohibition from teaching checks, section 128 direction checks, overseas criminal record checks where applicable, and verification of your full employment history including any gaps.

Where a separate Recruitment Privacy Notice is in force, it provides additional detail about how applicant data is processed before appointment. This notice covers processing from the point of appointment or engagement onwards, and it also covers recruitment records that are transferred into your personnel file.

3.2 Employment and engagement data

Throughout your employment or engagement we collect and process:

- your contract and terms of employment or engagement;
- payroll and pension information, including bank details, tax code and National Insurance number;
- next of kin and emergency contact details;

- attendance and absence records, including reasons for absence;
- performance management, supervision and appraisal records;
- training records and continuing professional development documentation;
- records relating to disciplinary or grievance proceedings;
- records relating to your ongoing suitability to work with children, including DBS Update Service checks, annual self-declarations relating to disqualification, references received, and your entry on the Single Central Record; and
- records in which you are named alongside a student, for example incident, accident, and safeguarding records.

3.3 Special category data

We process some special category data about our workforce under Article 9 of the UK GDPR. This includes:

- information about your physical or mental health, such as occupational health reports, fit notes and reasonable adjustment records;
- records of wellbeing support or supervision provided to you in connection with your role;
- information about disability, for the purpose of making reasonable adjustments;
- trade union membership, where you have authorised a payroll deduction; and
- equal opportunities monitoring data provided voluntarily by you.

3.4 Criminal offence data

Separately from special category data, we process criminal offence data within the meaning of Article 10 of the UK GDPR. This includes enhanced DBS certificate information, barred list, prohibition and section 128 check outcomes, DBS Update Service status checks, annual self-declarations relating to disqualification, and information disclosed to us about allegations, cautions or convictions.

We process criminal offence data only where we have both a lawful basis under Article 6 of the UK GDPR and a condition under Schedule 1 of the Data Protection Act 2018.

3.5 IT systems and records

We hold records generated by your use of school accounts and systems, including email and file access logs and entries you make in the systems we use for teaching, recording and safeguarding. We do not use these records to monitor individual staff performance as a matter of routine. Where we access them for any purpose other than routine system administration, it will be for a specific safeguarding, conduct, security or legal reason.

4. Why we use this data and our lawful basis

The table below sets out the main purposes for which we process workforce data, the lawful basis we rely on under Article 6 of the UK GDPR, and, where relevant, the condition we rely on for special category or criminal offence data under Schedule 1 of the Data Protection Act 2018.

Purpose	Lawful basis (Article 6)	Condition for special category or criminal offence data
Administering your contract, including pay, benefits and pension	Performance of a contract	Employment, social security and social protection (Schedule 1, Part 1, paragraph 1) where health data is involved
Safer recruitment checks and maintaining the Single Central Record	Legal obligation – Education (Independent School Standards) Regulations 2014, Safeguarding Vulnerable Groups Act 2006, KCSIE	Safeguarding of children and of individuals at risk (Schedule 1, Part 2, paragraph 18)
Managing absence, sickness and occupational health	Legal obligation – Employment Rights Act 1996 – and legitimate interests	Employment, social security and social protection (Schedule 1, Part 1, paragraph 1)
Performance management, supervision and appraisal	Performance of a contract and legitimate interests	Employment, social security and social protection (Schedule 1, Part 1, paragraph 1) where health data is involved
Disciplinary and grievance procedures	Legal obligation and legitimate interests	Employment (Schedule 1, Part 1, paragraph 1) and, where safeguarding is engaged, safeguarding (Schedule 1, Part 2, paragraph 18)
Ensuring health and safety at work	Legal obligation – Health and Safety at Work etc. Act 1974	Employment, social security and social protection (Schedule 1, Part 1, paragraph 1)
Meeting HMRC, tax and pension auto-enrolment obligations	Legal obligation	Not applicable
Training and continuing professional development	Performance of a contract and legitimate interests	Not applicable
Safeguarding and child protection, including managing allegations and low-level concerns	Legal obligation – Children Act 1989 and 2004, KCSIE – and recognised legitimate interest (safeguarding condition)	Safeguarding of children and of individuals at risk (Schedule 1, Part 2, paragraph 18)
Meeting our regulatory duties to the Independent Schools Inspectorate and the Department for Education	Legal obligation	Safeguarding of children and of individuals at risk (Schedule 1, Part 2, paragraph 18) where relevant
Equal opportunities monitoring	Consent	Explicit consent (Article 9(2)(a))

Purpose	Lawful basis (Article 6)	Condition for special category or criminal offence data
Establishing, exercising or defending legal claims	Legitimate interests	Legal claims (Schedule 1, Part 1, paragraph 33)

Where we rely on the recognised legitimate interests basis introduced by the Data (Use and Access) Act 2025, we are required to tell you which of the five recognised conditions applies. For More Than Ed this is the safeguarding condition in Annex 1 to the UK GDPR, which covers processing necessary to protect children and individuals at risk from neglect or from physical, mental or emotional harm. No balancing test is required for processing that falls within this condition, but you retain the right to object to it (see section 10).

Where we rely on consent, you may withdraw it at any time by contacting the Data Protection Lead. Withdrawing consent will not affect processing already carried out, and it will not disadvantage you. Providing equal opportunities monitoring data is entirely voluntary.

Some of the information we ask you for is required by law or is necessary in order to enter into your contract – for example your right to work documentation, DBS check and payroll details. If you do not provide it, we may not be able to appoint you or to continue your engagement.

5. How we collect your data

We collect most personal data directly from you, during recruitment and throughout your employment or engagement. We also receive data about you from:

- the Disclosure and Barring Service and the Teaching Regulation Agency;
- HMRC and our pension provider;
- occupational health and employee assistance providers;
- previous employers, in the form of references;
- the local authority designated officer (LADO), where an allegation is made;
- our outsourced HR, Safeguarding and Health and Safety advisers (Judicium); and
- professional and regulatory bodies.

6. Who we share your data with

We share your personal data only where it is necessary and lawful to do so. Recipients may include:

- HMRC, for tax and National Insurance purposes;
- our payroll provider and our pension provider;
- the Disclosure and Barring Service and the Teaching Regulation Agency;
- the local authority designated officer (LADO) and, where necessary, children's social care and the police, where a safeguarding allegation or concern is raised;

- the Independent Schools Inspectorate and the Department for Education, in connection with inspection and regulation;
- our outsourced HR, safeguarding and health and safety advisers;
- occupational health providers and the staff wellbeing service;
- our IT and software suppliers, who process data on our behalf;
- professional advisers, including solicitors, insurers and auditors;
- trade unions, where you are a member and have authorised a payroll deduction; and
- prospective employers, where you have named the school as a referee.

We do not sell personal data, and we do not share it for marketing purposes. Where a third party processes personal data on our behalf, we put a written contract in place that meets the requirements of Article 28 of the UK GDPR.

As an independent school, we are not required to submit the School Workforce Census, and we do not routinely provide workforce data to the Department for Education for that purpose.

7. Transfers outside the United Kingdom

Your personal data is normally held within the United Kingdom. Some of our IT and software suppliers may store or access data outside the UK. Where that happens, we ensure that a transfer mechanism recognised under Chapter V of the UK GDPR is in place – for example an adequacy regulation, the International Data Transfer Agreement, or the UK Addendum to the EU standard contractual clauses – and we satisfy ourselves that the protection given to your data is not materially lower than it would be under UK law. You can ask the Data Protection Lead for details of any transfer that affects you.

8. How long we keep your data

We retain workforce records in accordance with the IRMS Records Management Toolkit for Schools and Academies and with statutory guidance. In summary:

- personnel files and general training records are retained for six years after the end of your employment or engagement;
- training records relating to work with children, including safeguarding training, are retained for the longer period set out in the IRMS toolkit;
- payroll and tax records are retained for six years plus the current tax year;
- records of a safeguarding allegation against you, including where an allegation is unsubstantiated, are retained at least until you reach normal pension age, or for ten years from the date of the allegation, whichever is longer, in line with KCSIE;
- where an allegation is found to be false, unsubstantiated or malicious, it is not retained on your personnel file and is not referred to in any reference, in line with KCSIE;
- DBS certificate numbers and check dates are recorded on the Single Central Record and retained for the duration of your employment and for the period required for inspection purposes; DBS certificates themselves are not retained; and

- recruitment records for unsuccessful candidates are retained for six months from the date the decision is notified.

When personal data is no longer required, it is securely deleted or destroyed.

9. Data security

We take the security of your personal data seriously and have implemented appropriate technical and organisational measures to protect it. These include:

- restricting access to personal data so that it is available only to those who need it for their role;
- secure storage of physical personnel files;
- encryption and password protection for electronic records;
- regular review of access permissions;
- written contracts with all suppliers who process personal data on our behalf; and
- mandatory staff training on data protection and confidentiality.

We record all personal data breaches. Where a breach is likely to result in a risk to people's rights and freedoms, we report it to the regulator within 72 hours of becoming aware of it, and we tell affected individuals where the law requires us to.

10. Your rights

Under the UK GDPR you have the right:

- to be informed about how your data is used, which this notice is intended to fulfil;
- to access your personal data by making a subject access request (see section 11);
- to have inaccurate personal data corrected;
- to request erasure of your data in certain circumstances;
- to restrict processing in certain circumstances;
- to object to processing based on legitimate interests or recognised legitimate interests;
- to withdraw consent at any time, where we rely on consent; and
- to data portability in certain circumstances.

These rights are not absolute. Some are limited where we process data under a legal obligation, for safeguarding purposes, or in connection with legal proceedings. For example, we cannot delete records that we are legally required to retain, and safeguarding records cannot be amended or deleted at your request where retention is necessary to protect children.

If you wish to exercise any of these rights, please contact the Data Protection Lead.

11. Making a subject access request

You have the right to request a copy of the personal data we hold about you. Requests should be made to the Data Protection Lead, and we will accept a request made in writing in any form. We will respond within one calendar month.

Following the changes made by the Data (Use and Access) Act 2025, which took effect on 5 February 2026:

- the one-month period does not begin until we have received any information we reasonably need in order to respond, such as proof of identity or clarification of the scope of your request. Where we ask for that information, the time limit is paused until you provide it;
- we are required to carry out a reasonable and proportionate search, rather than an exhaustive one; and
- we may extend the period by up to a further two months where a request is complex or where you have made a number of requests, and we will tell you if we do.

We may need to redact information about other people, and we may withhold information that is subject to legal privilege or that is exempt under the Data Protection Act 2018 – including, in some circumstances, information given in confidence in connection with a safeguarding matter. We may refuse a request that is manifestly unfounded or excessive under Article 12(5) of the UK GDPR, and we will explain our reasons if we do so.

12. Automated decision-making and profiling

We do not make decisions about staff, volunteers or contractors by automated means alone.

The Data (Use and Access) Act 2025 replaced the previous general prohibition on solely automated decision-making with a framework of safeguards under Articles 22A to 22D of the UK GDPR. If we were ever to introduce solely automated decision-making with legal or similarly significant effects, we would tell you beforehand, and you would have the right to be given information about the decision, to make representations, to obtain human intervention, and to contest the decision. Solely automated decisions based on special category data continue to require your explicit consent or another condition under Article 9.

13. Data protection complaints

Since 19 June 2026, section 164A of the Data Protection Act 2018 has required us to make it straightforward for you to complain about the way we have handled your personal data.

If you are unhappy, please raise it with the Data Protection Lead in the first instance. We will acknowledge your complaint within 30 days of receiving it, and we will respond substantively without undue delay, telling you what we have done or what we intend to do.

You do not need to use the staff grievance procedure in order to make a data protection complaint, although you may choose to do so where the matter also concerns your employment.

14. Social media and online presence

Our expectations regarding staff use of social media are set out in our Staff Code of Conduct and Social Media Policy. We do not routinely monitor staff social media accounts, however, we may access publicly available information where there is a specific safeguarding or conduct concern, in accordance with our legal obligations and legitimate interests.

15. Changes to this notice

We may update this privacy notice from time to time to reflect changes in our practices or in the law. We will notify you of any significant change. The current version is available on our website and from the school office, and it is also drawn to your attention at induction and on renewal of your contract or agreement.

16. Contact and complaints to the regulator

If you have any questions about this privacy notice or about how we handle your personal data, please contact our Data Protection Lead, Jonathan Munda, at jonathan.munda@mted.uk or by writing to More Than Ed Independent School, Cherry Tree Court, Woodfield Park, Balby, Doncaster, DN4 8QN.

We would normally expect you to raise a concern with us first (see section 13). If you are not satisfied with our response, you have the right to complain to the Information Commissioner's Office at www.ico.org.uk or by telephone on 0303 123 1113.

Under the Data (Use and Access) Act 2025, the Information Commissioner's Office is being reconstituted as the Information Commission. References in this notice to the Information Commissioner's Office should be read as references to the Information Commission once the transfer of functions is complete.

You also have the right to seek a remedy through the courts.

17. Related policies

This notice should be read alongside the school's other policies and documents, including:

- Data Protection Policy
- Recruitment Privacy Notice
- Privacy Notice – Students, Parents and Carers
- Records Management and Retention Schedule
- Personal Data Breach Procedure
- Information Security and Acceptable Use Policy
- Safer Recruitment Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Social Media Policy
- Health and Safety Policy

- Grievance Procedure

18. Legislation and guidance

In drawing up this notice, the school has had regard to the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Keeping Children Safe in Education (Department for Education), in force 1 September 2026
- Education (Independent School Standards) Regulations 2014
- Safeguarding Vulnerable Groups Act 2006
- Children Act 1989 and Children Act 2004
- Employment Rights Act 1996
- Health and Safety at Work etc. Act 1974
- Equality Act 2010
- IRMS Records Management Toolkit for Schools and Academies
- ICO guidance on recognised legitimate interests, the right of access, and data protection complaints