ALTRINCHAM PREPARATORY SCHOOL

Data Protection Policy

Author:	Mrs Denise Barber – Business Operations Manager
Responsible Person:	Mr Nick Vernon–Headmaster
Date of last review:	June 2026 (D Barber)
Summary of changes:	To comply with the Data Use and Access Act 2025, including the new right to complain
Date of next review:	June 2027

1. BACKGROUND

Data protection is an important legal compliance issue for Altrincham Preparatory School (the "School"). During the course of the School's activities we collect, store and process personal data (sometimes sensitive in nature) about staff, pupils, their parents, contractors and other third parties (in a manner more fully detailed in our Privacy Notice). We, as the data "controller", are liable for the actions of our staff and directors/governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK GDPR") and the Data Protection Act 2018 ("DPA 2018"), as supplemented and amended by the Data (Use and Access) Act 2025. The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office ("ICO**"**) is responsible for enforcing data protection law in the UK, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. DEFINITIONS

Key data protection terms used in this data protection policy are:

- **[Data] Controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including its directors/governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.

- **[Data] Processor** – an organisation that processes personal data on behalf of a controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- **Personal information (or 'personal data'):** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

- **Processing** – virtually anything done with personal data, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

- **Special categories of personal data –** data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3. APPLICATION OF THIS POLICY

This policy sets out our expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors/directors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where we share personal data with third party controllers – which may range from other schools, to parents, to appropriate authorities – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

4. PERSON RESPONSIBLE FOR DATA PROTECTION AT THE SCHOOL

We have appointed Mr Nick Vernon as the Data Protection Co-ordinator who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Co-ordinator.

5. THE PRINCIPLES

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and processors). These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specific and explicit purposes and only for the purposes it was collected for
3. Relevant and limited to what is necessary for the purposes it is processed
4. Accurate and kept up to date
5. Kept for no longer than is necessary for the purposes for which it is processed
6. Processed in a manner that ensures appropriate security of the personal data

The UK GDPR's broader 'accountability' principle also requires that we not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. LAWFUL GROUNDS FOR DATA PROCESSING

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable that we rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, in most cases it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means that we are taking on extra responsibility for considering and protecting people's rights and interests. Our legitimate interests are set out in its Privacy Notice, as the UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity

- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

7. HEADLINE RESPONSIBILITIES OF ALL STAFF

Record-keeping

It is important that personal data we hold is accurate, fair and adequate. You are required to inform the School if you believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how you record your own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

You should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage you from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is that you record every document or email in a form you would be prepared to stand by should the person about whom it was recorded ask to see it.

Data handling

You have a responsibility to handle the personal data which you come into contact with fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to you). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so you should read and comply with the following policies:

- Child Protection and Safeguarding
- IT Acceptable Use
- Bring your own device
- Social media
- Taking, storing and using images of children

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, we must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must notify Mr Nick Vernon, Headmaster. If you are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but we always need to know about them to make a decision.

As stated above, we may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Care and data security

More generally, we require you (and expect all our contractors) to remain mindful of the data protection principles (see section 3 above), and to use your best efforts to comply with those principles whenever you process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how we use personal information to Mr Nick Vernon, Headmaster, and to identity the need for (and implement) regular staff training. You must attend any training we require you to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including most uses of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to Mr Nick Vernon, Headmaster, in the first instance, and at as early a stage as possible.

8. RIGHTS OF INDIVIDUALS

In addition to responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell Mr Nick Vernon, Headmaster, as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate
- request that we erase their personal data (in certain circumstances)
- request that we restrict our data processing activities (in certain circumstances)
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller;
- complain to us about a data protection issue (eg if they are unhappy with the response to their subject access request or how we have collected or used their personal information)
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.
- contest or seek human intervention in cases of solely automated individual decision-making (i.e. where a significant decision is made about the individual without human intervention)
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

The above rights for individuals are generally subject to exceptions or exemptions rather than functioning as absolute rights and so they do require careful assessment before the school responds.

If you receive a request from an individual who is purporting to exercise one or more of their data protection rights, or making a complaint about something data protection related, you must tell Mr Nick Vernon, Headmaster, as soon as possible as these rights are subject to statutory requirements including as regards the timeframes for responding.

9. DATA SECURITY: ONLINE AND DIGITAL

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- You are not permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Headmaster.
- You should not provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Use of personal email accounts or personal devices by governors or staff for official School business is not permitted.

10. PROCESSING OF FINANCIAL DATA

Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

11. SUMMARY / POLICY STATEMENT

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

Appendix One – Appropriate Policy Document (APD)

Introduction

Altrincham Preparatory School processes special category and criminal conviction data in the course of fulfilling its functions as a school. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This policy complements our existing records of processing as required by Article 30 of UK General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces our existing retention and security policies, procedures and other documentation in relation to special category data.

Special categories and conditions of processing

We process the following special categories (SC) of data:

- racial or ethnic origin,
- religious or philosophical beliefs,
- health,
- sex life/orientation,

We also process criminal offence (CO) data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations.

We rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Article 9(2)(a) – explicit consent
We make sure that consent given by any person is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing. We regularly review consents to ensure they remain up to date.

Examples of such processing includes when we ask for health or medical information from visitors to aid them in the event of an emergency.

Article 9(2)(b) – employment, social security or social protection
To comply with our legal requirements as an employer and safeguard our pupils, we need to collect some special category data.

Examples include when we carry out DBS checks on staff to evidence suitability for a role; collect medical information to put in reasonable adjustments at work and monitor staff absence.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we rely on for this processing is **Schedule 1, Part 1, (1) - employment, social security and social protection.**

Article 9(2)(g) – reasons of substantial public interest
We have a wide variety of duties we must carry out in the public interest. Much of our processing of SC data is done so for the purposes of substantial public interest.

Examples include when we process SC data to identify pupils who require additional support such as special educational needs; processing safeguarding concerns to ensure the safety and wellbeing of pupils; or collecting medical information when monitoring pupil attendance or dietary requirements.

When processing data under Article 9(2)(g), we also require a Schedule 1 condition under the Data Protection Act 2018. The conditions we rely on for this processing are **Schedule 1, Part 2, (6) – statutory and government purposes; (10) – preventing or detecting unlawful acts; and (18) – safeguarding of children and of individuals at risk.**

Compliance with Data Protection Principles
We have several policies and procedures in place to ensure our compliance with the Article 5 Data Protection Principles and meet our accountability obligations, explained in more detail below:

Accountability principle
We have put in place appropriate technical and organisational security measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Co-ordinator, Nick Vernon.
- Taking a data protection by design and default approach to our processing activities, including the use of risk assessments.
- Maintaining documentation of our processing activities through an Information Asset Register.
- Adopting and implementing information governance policies and ensuring we have written contracts in place with data processors.
- Implementing appropriate security measures in relation to the personal data we process. More detail can be found in our Information Security Policy.

Principle (a): lawfulness, fairness and transparency
Processing personal data must be lawful, fair and transparent. We have identified an appropriate Article 6 condition and also, where processing SC or CO data, an Article 9 and Schedule 1 condition.

We consider how any processing may affect individuals concerned and provide clear and transparent information about why we process personal data, including our lawful bases, in our privacy notices and this policy document. All privacy notices provide details of data subject rights. Our privacy information is regularly reviewed and updated to ensure it accurately reflects our processing.

Principle (b): purpose limitation
Schools can only act in ways and for purposes which they are empowered to do so by law. Personal data is therefore only processed to allow us to carry out the necessary functions and services we are required to provide in line with

legislation. We clearly set out our purposes for processing in our privacy notices, policies and procedures, and in our IAR. If we plan to use personal data for a new purpose, other than a legal obligation or function set out in law, we check that it is compatible with our original purpose, or we obtain specific consent for the new purpose.

Principle (c): data minimisation
We only collect the minimum personal data needed for the relevant purposes, ensuring it is necessary and proportionate. Any personal information that is no longer required, especially where it contains special category data, is anonymised or erased. Further information can be found in our Records Management Policy.

Principle (d): accuracy
Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is processed, we will take every reasonable step to ensure that data is erased or rectified without delay. Where we are unable to erase or rectify the data, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision. Where we have shared information with a third party, we will take all reasonable steps to inform them of the inaccuracies and rectification. We maintain a log of all data rights requests and have appropriate processes for handling such requests.

Principle (e): storage limitation
We have a Retention Schedule in place which is based on guidance issued by the Information and Records Management Society (IRMS). Where there is no legislative or best practice guidance in place, the Headmaster will decide how long the information should be retained based on the necessity to keep the information for a legitimate purpose or purposes. We also maintain a Destruction Log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed. Further information can be found in our Records Management Policy.

Principle (f): integrity and confidentiality (security)
We employ various technical and organisational security measures to protect the personal and special category data that we process. A full description of security measures can be found in our Information Security Policy.

In the event of a personal data breach the incident will be recorded in a log, investigated, and reported to our Data Protection Co-ordinator where necessary. High risk incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in our Information Security Policy.

Retention of special category and criminal convictions data
The retention periods of special category and criminal convictions data are set out in our Retention Schedule. Retention periods of specific information assets are identified in our Information Asset Register and we have in place a Records Management Policy.