South Manchester Learning Trust

Trust Wide Policy

Data Protection Policy

Date of Board Approval: May 2023
Date of Review: May 2024

South Manchester Learning Trust

Contents

1. **Introduction** 1
2. **Responsibilities** 2
   - **2.2. Data Protection Officer responsibilities** 2
   - **2.3. Staff responsibilities** 2
3. **Data Protection Principles** 3
4. **The lawful basis for processing** 3
5. **Accountability** 4
6. **Data protection by design and default** 4
7. **Data Protection Impact Assessment** 5
8. **Rights of the data subject** 5
9. **Data Protection Breaches** 8
10. **Consent** 9
11. **CCTV – [remove if school does not use CCTV]** 9
12. **Photography** 9
13. **Data sharing** 10
14. **Data Security and Storage of Records** 10
15. **Disposal of records** 11
16. **Training** 11
17. **Glossary of Terms** 11

1. Introduction

South Manchester Learning trust (Altrincham College & Reddish Vale) takes its responsibilities with regards to the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) seriously. This policy sets out how the school manages those responsibilities.

Altrincham College & Reddish Vale High School are committed to data protection by design and regards the lawful and appropriate processing of personal and special category data as an integral part of its purpose.

This policy sets out the accountability and responsibilities of the school, its staff and its students to comply fully with the provisions of UK GDPR and DPA.

Altrincham College & Reddish Vale High School holds and processes personal data about individuals such as employees, students and others, defined as 'data subjects'. Such data must only be processed in accordance with UK GDPR and the DPA.

This policy therefore seeks to ensure that we:

1. Protect personal data and the rights and freedoms of the data subject
2. Are clear about how personal data must be processed and the school's expectations for all those who process personal data on its behalf
3. Comply with the data protection laws, guidance and good practice
4. Protect the school's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
5. Protect the school from risks of personal data breaches and other breaches of data protection law.

This policy applies to all personal data the school processes regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the school's behalf must read it. A failure to comply with this policy may result in disciplinary action.

The school has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with UK GDPR and the DPA.

2. Responsibilities

2.1. School responsibilities

The school, as data controller is responsible for establishing policies and procedures in order to comply with data protection.

The Data Protection (Charges and Information) Regulations 2018 requires every data controller (i.e. organisation) in the UK to pay a fee to the Information Commissioner's Office (ICO). The school's registration number is ZA276100.

2.2. Data Protection Officer responsibilities

The DPO is responsible for:

- Advising the school and its staff of its obligations under UK GDPR;
- Monitoring compliance with the UK GDPR and other relevant data protection law, the school's policies with respect to this, and monitoring training and audit activities related to UK GDPR compliance;
- To provide advice where requested on data protection impact assessments;
- To cooperate with and act as the contact point for the ICO;
- The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

2.3. Staff responsibilities

Staff members who process personal data about students, staff, applicants or any other individual must comply with the requirements of this policy. Staff members must ensure that:

- All personal data is kept securely;
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Personal data is kept in accordance with the school's retention schedule
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Governance Team
- Any data protection breaches are swiftly brought to the attention of Senior Managers and in turn the Information Governance team;

- All mandatory data protection training is completed and refreshed annually.

If staff are unsure about who are the authorised third parties to whom they can legitimately disclose personal data, they should seek advice from the Business Manager and Senior Leadership Team.

3. Data Protection Principles

The UK GDPR is based on data protection principles that the school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data,

This Policy sets out how South Manchester Learning trust aims to comply with these principles.

4. The lawful basis for processing

The first principle requires all personal data to be processed lawfully, fairly and in a transparent manner. We will only process personal data where we have one of six 'lawful bases' to do so under data protection law:

1. **Consent:** the individual has given clear consent for the school to process their personal data for a specific purpose.
2. **Contract:** the processing is necessary for a contract the school has with the individual, or because they have asked us to take specific steps before entering into a contract.
3. **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
4. **Vital interests:** the processing is necessary to protect someone's life.

5. **Public task**: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
6. **Legitimate interests:** the processing is necessary for the school's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

For special categories (see glossary) of personal data, we will also meet one of the special category conditions for processing, which are set out in the UK GDPR and Data Protection Act 2018.

5. Accountability

The school must implement and evidence appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. To demonstrate this, the school has implemented the following:

- Appointed a suitably qualified DPO.
- Implemented Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects (further information may be found below).
- Integrated data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches.
- Trained staff on compliance with Data Protection and keeping records accordingly.
- Regular testing of the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

6. Data protection by design and default

Under UK GDPR, the school has an obligation to consider the impact on data privacy during all processing activities. There is an obligation to consider the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons. The school will ensure that:

- Appropriate technical and organisational measures are implemented to minimise the potential negative impact processing can have on the data subjects' privacy.

- Senior managers understand their responsibility for ensuring there is a privacy culture within the school and ensure policies and procedures are developed with Data Protection in mind.
- Privacy and data protection issues are always considered at the design phase of any system, service, product or process.
- Only data that is necessary to achieve a specific purpose is processed. This links to the fundamental data protection principles of data minimisation and purpose limitation.

7. Data Protection Impact Assessment

When considering new processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) will be conducted. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection requirements are not an after-thought.

A DPIA will be completed (and findings discussed with the DPO) in the following circumstances:

- The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated processing including profiling;
- Large scale processing of sensitive (special category) data; and
- Large scale, systematic monitoring of a publicly accessible area.

8. Rights of the data subject

UK GDPR was designed to strengthen the privacy rights of individuals. It offers more control to the data subject over what happens to their personal data. This has been expressed in UK GDPR under the following eight rights:

The Right to be informed

The right to be informed covers some of the key transparency requirements of GDPR, namely the first principle which promotes fair and transparent processing of personal data. Essentially, it' is about being as clear and concise as possible with the data subject and informing them how and why their information is being used.

Data subjects have the right to receive a copy of their personal data which is held by the School. In addition, an individual is entitled to receive further information about the School's processing of their personal data as follows:

1. The purposes

2. The categories of personal data being processed

3. Recipients/categories of recipient

4. Retention periods

5. Information about their rights

6. The right to complain to the ICO

7. Details of the relevant safeguards where personal data is transferred outside the EEA

8. Any third-party source of the personal data

The Right of Access

The right of access, commonly referred to as subject access, essentially gives individuals the right to obtain a copy of all their personal information. It helps individuals to understand how and why you are using their data, and also to check you are doing so lawfully.

The Right to Rectification

The right to rectification allows an individual to have any inaccurate information rectified. An individual may also be able to have incomplete personal data completed, although this depends on the purposes for the processing. This is closely linked to the 'Accuracy' principle of GDPR, however, although steps may have been taken to ensure that personal data was accurate when you obtained it, this right requires reconsideration of the accuracy upon request.

The Right to Erasure

The right to erasure, commonly referred to as, 'the right to be forgotten', gives individuals the right to have their personal data erased. However, this is not an absolute right and only applies in certain circumstances. A few examples of instances where it could apply would be:

I. If the personal data is no longer necessary for the purpose for which it was originally collected;

II. If ‘consent’ is the lawful basis for holding the data, and the individual withdraws their consent; and
III. You have processed the personal data unlawfully.

The Right to Restrict Processing

This right allows an individual to restrict the processing of their data. This means they can limit the way an organisation uses their data, and can be thought of as an alternative to requesting the erasure. Similarly, this can only be applied in certain circumstances such as:

I. When the individual contests the accuracy of their personal data and you are in the process of verifying this accuracy;
II. The data has been processed unlawfully, and instead of erasure, the individual request restriction instead; and
III. You no longer need the personal data, but the individual requests you keep it in order to establish, exercise or defend a legal claim.

The Right to Data Portability

The right to data portability gives individuals the right to have any data they have provided to a controller to be moved between data controllers. This right only applies when the lawful basis for processing the information is either consent or for the performance of a contract. It also only applies to processing carried out digitally (i.e. this excludes paper files). The definition of ‘provided to a controller’ doesn’t just mean direct information given to the controller, it can also mean personal data resulting from observation of an individual’s activities.

This may include:

I. History of website usage or search activities;
II. Traffic and location data; or
III. ‘Raw’ data processed by connected objects such as smart meters and wearable devices.

The Right to Object

This gives individuals the right to object to the processing of their personal data, effectively asking the organisation to stop processing it. Again, this can only be used in certain circumstances and depends on the purposes and lawful basis used for processing.

An example of when this right can be applied is when:

Personal data is being used for direct marketing purposes and the individual wishes to object to this.

However, this right isn't absolute and will need to be carefully weighed up between the organisations' justification for processing the information, and the rights and freedoms of the individual.

The Rights to Automated Decision Making

GDPR has provisions on decisions which are made solely by automated means without any human involvement, and profiling (automated processing of data to evaluate certain things about an individual).

Examples of this would be:

I. An online decision to award a loan.
II. Or a recruitment aptitude test which uses pre-programmed algorithms and criteria.

GDPR restricts you from making solely automated decisions, included those based on profiling, that have a legal or similarly significant effect on an individual. The type of effect isn't specifically defined in GDPR however the decision must have a serious negative impact on an individual to be under the remit of this provision.

Altrincham College and Reddish Vale High School has an individual Data Subject Rights Policy.

9. Data Protection Breaches

Altrincham College & Reddish Vale High School are responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. Potential incidents include

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any suspected data protection incident will be brought to the attention of the school's Information Governance Team and DPO, who will investigate and decide if the incident constitutes a data protection breach.

If a reportable data protection breach occurs, the school is required to notify the ICO as soon as possible, and no later than 72 hours after becoming aware of it. Any

member of the school who encounters something they believe may be a data protection incident must report it immediately.

10. Consent

UK GDPR sets a high standard for consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement between the school, parents and pupils.

UK GDPR is clear that an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service.

Altrincham College & Reddish Vale High School will keep clear records to demonstrate where consent has been given.

11. CCTV – [remove if school does not use CCTV]

Altrincham College & Reddish Vale High School understands that recording images of identifiable individuals is processing personal information and must be done in line with data protection principles.

The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via the Privacy Notice.

All CCTV footage will be kept for 30 days for security purposes.

For more information regarding how we use CCTV please view our CCTV Policy on the school website: https://www.altrinchamcollege.com/.

12. Photography

Altrincham College & Reddish Vale High School takes images/video footage of pupils throughout their school life. Photographs/video footage often consist of personal data and must be managed under data protection principles.

The school ensures it gathers [parent/pupil] consent in order to process images of pupils for school purposes such as, internal displays, school website, prospectus, or recordings of school plays.

Images captured by individuals for their domestic purposes, and videos made by parents for family use, fall outside the scope of UK GDPR.

A consent form for the particular usage of images will be sent to parents [annually/when the pupil starts at the School].

13. Data sharing

Altrincham College & Reddish Vale High School will usually only share data with third parties when they have a legal or statutory obligation or have the consent of parents/pupils.

Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- Establish a data sharing agreement (see with the supplier or
- contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

14. Data Security and Storage of Records

Altrincham College & Reddish Vale High School will aim to protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and servers that contain personal data are kept locked away when not in use.

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to choose strong passwords and never reveal their passwords to others.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Altrincham College & Reddish Vale High School only keeps personal data for as long as is required under legislation or business need. The School refers to a records retention schedule to determine when records no longer need to be retained.

Once personal data is no longer needed it is confidentially disposed of using secure methods.

16. Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of staff members' continuing professional development, on an annual basis.

17. Glossary of Terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data is data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controller means the person/business who determines the purposes for which personal data will be processed, and the manner in which it will be processed.

Data processor means the person/business that processes personal data on behalf, and in accordance with the instructions, of a data controller.

Special category data includes information about a person's race, ethnic origin, political opinions, religion, trade union membership, genetics, Biometrics (where used for ID), health, sexual life, or Sexual orientation.

Consent is an agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data Protection Officer (DPO) is the person appointed as such under UK GDPR. A DPO is responsible for advising the School on their obligations under Data Protection, for monitoring compliance with data protection law, as well as with the Schools polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

Personal Data Breach is any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Data Protection by Design and Default involves implementing appropriate technical and organisational measures in an effective manner to ensure compliance with UK GDPR.