UK DATA PROTECTION POLICY 2024

Date of Review	*May 2024*
Date reviewed by Governors /trustees	*8th May 2024*
Cycle of review	Annual

Agate Momentum Trust

Data Protection Policy

The Agate Momentum Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with its schools. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that its schools comply with its statutory obligations.

Our Commitment:
The Agate Momentum Trust and its schools are committed to the protection of all personal and sensitive data for which they hold responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA). https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Changes to data protection legislation (UK GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows –

(a) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations).

(b) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(c) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.

The members of staff responsible for data protection are mainly:

- Keri Edge, Chief Executive Officer
- Sonu Somra Agate Momentum Trust Schools Business Manager
- Kelly Jones and Farhathhafza Quayyum, Heads of School.
- Sean Hearn, Federation ICT Network Manager

However, all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

The Trust is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them through within the school's annual professional development programme. The requirements of this policy are mandatory for all staff employed by Trust Schools and any third party contracted to provide services within the school.

Notification:
Our data processing activities are registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO: https://ico.org.uk/ESDWebPages/Search

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register. Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:
All data within our school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and that access to it does not breach the rights of the individuals to whom it relates. The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

The principles of the Data Protection Act shall be applied to all data processed:
• ensure that data is fairly and lawfully processed
• process data only for limited purposes
• ensure that all data processed is adequate, relevant and not excessive
• ensure that data processed is accurate
• not keep data longer than is necessary
• process the data in accordance with the data subject's rights
• ensure that data is secure
• ensure that data is not transferred to other countries without adequate protection.

Privacy Notices:
We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation. https://ico.org.uk/for-organisations/accountability-framework/transparency/
There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.
The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Privacy Notices can be found on school websites.

Data Security:
In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance. The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

For specific information related to the security of data held on the school's IT system including pupil use please refer to these policies:

- Acceptable Use Policy
- Infringement of the online safety policy
- Online Safety Policy
- Information and security policy

Data Access Requests (Subject Access Requests):
All individuals whose data is held by us, have a legal right to request access to such data or information about what is held. We shall respond to such requests within one calendar month and they should be made to the School Business Manager at Hallsville Primary School or Scott Wilkie Primary School either in writing at:

- Hallsville Primary School, Radland Road, Canning Town, London E16 1LN
- Scott Wilkie Primary school, Hoskin's Close, London E16 3HD

by email: info@hallsville.newham.sch.uk/info@scottwilkie.newham.sch.uk
by telephone: 0207 476 2355/0207 474 4138
or in person.

There is usually no charge to access such information unless the request is excessive in which case schools may charge up to £10 to provide it.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in order to perform a public task in the public interests. Data may be disclosed to the following third parties without consent:

The pupil's family and representatives

to perform a public task in the public interests in order to carry out our official functions for example reporting on pupil progress.

Other schools

If a pupil transfers from an Agate Momentum Trust School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Our local authority

to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions

The Department for Education

to meet our legal obligations to share certain information with it, such as test outcomes.

Examination authorities

This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

Health authorities

As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

Police, Courts and Tribunals

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Social workers and support agencies

In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Suppliers and service providers

to enable them to provide the service we have contracted them to do for example BROMCOM MiS so we can carry out our public tasks for example registers and attendance details.

Survey and research organisations

to perform a public task in the public interests for example contributing to international pupil performance research such as PISA (Programme for International Student Assessment) which enables us to evaluate our effectiveness and challenges us to continue developing best practice.

Security organisations

to perform a public task in the public interests such as digitsing the signing in system in order to keep the school safe.

Professional advisers and consultants

to perform a public task in the public interests in order, for instance, to evaluate our effectiveness, support and challenge school leaders and continue developing best practice.

Charities and voluntary organisations

to perform a public task in the public interests in order, for instance, to implement resilience programmes through the charity Head Start.

Professional bodies

to perform a public task in the public interests in order, for instance sharing best practice across schools in order to promote best practice and raise pupil attainment.

Right to be Forgotten:
Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors.

Photographs and Video:
Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.
Where photographs/digital imagery are taken solely for personal use e.g. parents taking photographs in a school concert or sports day this will continue to be permitted. Where photographs are for personal use only the UK GDPR does not apply.
Parents/staff/members of the public will be reminded that it is not permissible to share such images on social media (See Consent Policy).

Location of information and data:
Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored with the school medical coordinator.
Sensitive or personal information and data should not be removed from the school site; however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on school visits with pupils.
The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:
• Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places or left unattended under any circumstances.
• Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
• Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
• If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
• If it is necessary to use data away from the school it should be accessed through the cloud environment.

• Expectations relating to the safe storage & processing of digital data are explicitly outlined within the school's Information and security policy

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:
The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.
All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.
Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/records-management-and-security/
The school has identified a qualified source for disposal of IT assets and collections.
The school also uses Restore Datashred to dispose of sensitive data that is no longer required