DATA PROTECTION POLICY 2018

Date of Development: May 2018
Date Agreed by Governors:
Review Date: May 2020

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 compliance with all relevant data protection laws in respect of personal data and to protecting the "rights and freedoms" of individuals whose information the School collects in accordance with the General Data Protection Regulation (GDPR) and other related data protection laws. To that end, the School has developed, implemented, maintains and continuously improves data protection policies and procedures.
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

Responsibilities:

- The School is a data controller and a data processor under the GDPR.
- The Head Teacher and all those throughout the School who are responsible for developing and encouraging good information handling practices.
- The Data Protection Officer (DPO), a role specified in the GDPR, is accountable for ensuring that compliance with data protection legislation and good practice can be demonstrated.

  This accountability includes:
  1. Development and implementation of the GDPR as required by this policy; and
  2. Security and risk management in relation to compliance with the policy.

- The School's nominated person has been appointed to take responsibility for the School's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the School complies with the GDPR, as do staff in respect of data processing that takes place within their area of responsibility.
- The School's nominated person has specific responsibilities in respect of procedures such as the Subject Access Request (SAR) Procedure and is the first point of call for staff seeking clarification on any aspect of data protection compliance before contacting the Head Teacher.
- Compliance with data protection legislation is the responsibility of all members of the School who process personal information.
- The School will ensure appropriate data protection training is provided for all staff.
- Staff are responsible for ensuring that any personal data supplied by them, and that is about them, to the School is accurate and up-to-date.

The members of staff responsible for data protection are mainly:

- Keri Edge, Chief Executive Officer
- Hannah Cleland, Agate Momentum Trust Schools Business Manager
- Lorraine Johnson and Farhathhafza Quayyum, Heads of School.
- Nigel Mark, Federation ICT Network Manager

Objectives

- The School is committed to complying with data protection legislation and good practice including:
- Processing personal information only where this is strictly necessary for legitimate purposes
- Collecting only the minimum personal information required for these purposes and not processing excessive personal information
- Providing clear information to individuals about how their personal information will be used and by whom
- Only processing relevant and adequate personal information
- Processing personal information fairly and lawfully
- Maintaining an inventory of the categories of personal information processed by the School
- Keeping personal information accurate and, where necessary, up to date
- Retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate purposes
- Respecting individuals' rights in relation to their personal information, including their right of subject access
- Keeping all personal information secure
- Only transferring personal information outside the European Union in circumstances where it can be adequately protected
- The application of the various exemptions allowable by data protection legislation

ICO Registration:

- The School has notified the Information Commissioner's Office (ICO) that it is a data controller and that it processes certain information about data subjects. The School has identified all the personal data that it processes and this is contained in the Information Asset Register (IAR)
- A copy of the ICO Registration is retained by the Head Teacher and is available to view on the ICO website https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/
- The ICO registration is renewed annually
- The School's nominated person is responsible, each year, for reviewing the details of registration, in the light of any changes to the School's activities (as determined by changes to the IAR) and to any additional requirements identified by means of data protection impact assessments

The policy applies to all staff and interested parties of the School such as data processors. Any serious breach of data protection legislation will be dealt with under the School's disciplinary policy and may also be a criminal offence, in which case the matter will be reported to the Information Commissioner's Office (ICO) or Police. The School is required to report serious data breaches within 72 hours of the incident to the ICO.

When a personal data breach has occurred, the School will establish the likelihood and severity of the resulting risk to individual's rights and freedoms. If it is likely that there will be a risk the ICO must be notified.

Recital 85 of the GDPR explains that…"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Introduction to GPDR:
The GDPR replaces the EU (European Union) Data Protection Directive of 1995 and supersedes the Data Protection Act 1998. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and that it is processed lawfully.

Definitions:
Territorial scope – the GDPR applies to all controllers that are established in the EU who process the personal data of data subjects. It applies to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behaviour to data subjects who are resident in the EU.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative center. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. The School is a data controller.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – The GDPR does not define the age at which a person is considered to be a child. The processing of personal data of a child under 13 years of age in relation to online services is only lawful if parental or guardian consent has been obtained.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Risk assessment:
Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, the School shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The School has a process for assessing the level of risk to individuals associated with the processing of their personal information. The assessment is known as a Data Protection Impact Assessment (DPIA). The School shall manage any risks which are identified by the DPIA in order to reduce the likelihood of a non-conformance with this policy.

Where, as a result of a DPIA, it is clear that the School is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not the School may proceed must be escalated for review to the Head Teacher.

The DPO will, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the School's documented risk acceptance criteria and the requirements of the GDPR.

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/keydefinitions/

Data Protection Principles:
All processing of personal data must be done in accordance with the following data protection principles of the GDPR and the School's policies and procedures are designed to ensure compliance with them.

Personal data must be processed lawfully, fairly and transparently

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language commonly in the form of a privacy notice.

The specific information that must be provided to the data subject must as a minimum include:

- The contact details of the School
- The contact details of the DPO
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing

- Who the personal data will be shared with
- The period for which the personal data will be stored
- The existence of the data subject rights
- The categories of personal data concerned
- Is the data transferred out of the EU
- Any further information necessary to guarantee fair processing

Personal data can only be collected for specified, explicit and legitimate purposes

- Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of the School's GDPR registration.

Personal data must be adequate, relevant and limited to what is necessary for processing

- The School's nominated contact is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.
- All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Head Teacher
- The Head Teacher will review data collection methods on a regular basis to ensure that collected data continues to be adequate, relevant and not excessive.
- If data is given or obtained that is excessive or not specifically required by the School's documented procedures, the School's nominated contact is responsible for ensuring that it is securely deleted or destroyed in line with the School's retention schedule.

Personal data must be accurate and kept up to date

- Personal Data that is processed must be reviewed and updated as necessary. No data should be retained unless it is reasonable to assume that it is accurate.
- The Head Teacher is responsible for ensuring that all staff members are trained in the importance of collecting accurate data and maintaining it.
- It is also the responsibility of individuals to ensure that data held by the School is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate at the date of submission.
- Staff/Pupils/Others should notify the School of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained on the School's website. It is the responsibility of the School to ensure that any notification regarding change of circumstances is noted and acted upon within 1 month.
- The Head Teacher is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.
- The School's nominated contact will review all the personal data maintained by the School on a regular basis, by reference to the IAR, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed in line with School's data retention schedule.
- The School's nominated contact is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, for information about them that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

- Where personal data is retained beyond the processing date, it will be held securely in order to protect the identity of the data subject in the event of a data breach.
- Personal data will be retained in line with the School's Records Retention Schedule and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

Personal data must be processed in a manner that ensures its 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/principle-7-security/
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2014/02/privacyimpact-assessments-code-published/
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

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Data held by the School is secure, controlled and managed. The School's systems and network are regularly independently tested.

Security controls may be subject to audit and review by independent auditors.

Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

Safeguards

An assessment of the adequacy by the data controller taking into account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination, of the information
- How the information will be used and for how long
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations
- The security measures that are to be taken as regards the data in the overseas location

Accountability

The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform DPIAs, comply with requirements for prior notifications, or approval from the ICO and appoint a DPO.

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/guide-to-data-protection/privacy-noticestransparency-and-control/
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.

See Privacy Notices – Appendix 1

Data Access Requests (Subject Access Requests):
All individuals whose data is held by us, have a legal right to request access to such data which is held by the School in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the School,

and information obtained from third parties about that person. We shall respond to such requests within one calendar month and they should be made to the Trust School Business Manager, Hannah Cleland either in writing at: Agate Momentum Trust, Hallsville Primary School, Radland Road, Canning Town, London E16 1LN
by email: Hannah.cleland@scottwilkie.newham.sch.uk
by telephone: 0207 474 4138/0207 476 2355
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 subjects' rights
Data subjects have the following rights regarding personal data that is recorded about them:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

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 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.

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/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf
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

Consent

The School understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

The School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the School using standard consent documents e.g. when a new member of staff signs a contract of employment, or during induction for participants on programmes.

Where the School provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

Security of data

All Staff are responsible for ensuring that any personal data which the School holds and for which they are responsible, is kept securely and is not under any condition disclosed to any third party unless that third party has been specifically authorised by the School to receive that information and has entered into a confidentiality agreement.

Any third parties working with or for the School, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by the School without having first entered into an agreement which imposes on the third party obligations no less onerous than those to which the School is committed, and which gives the School the right to audit compliance with the agreement.

All personal data should be accessible only to those who need to use it. The School will form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a locked room with controlled access
- In a locked drawer or filing cabinet
- If computerised, password protected
- Encrypted if stored on mobile/removable devices

Care must be taken to ensure that PC screens and terminals are not visible except to authorised members of staff of the School.

Manual records are not to be left where they can be accessed by unauthorised personnel and may not be removed from School premises without explicit authorisation.

Personal data will only be deleted or disposed of in line with the School's Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Storage drives of redundant PCs and mobile devices are to be removed and immediately securely destroyed.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site and appropriate security controls implemented.

Security controls may include:

- Data encryption
- Password or PIN protected data
- Secure storage device
- Secure remote access to the data
- Not working in an environment that is not secure or safe
- Not keeping laptops or paper records overnight in a vehicle

Disclosure of data
The School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the School's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left the School, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. The School's Retention Procedure will apply in all cases.

We keep our records in line with the retention guidelines for schools recommended by the Information and Records Management Society: https://ico.org.uk/ / http://ldbsact.org/download/policies/Document%20Retention%20Schedule_Nov15.pdf

Compliance
All staff are expected to comply with the School's policies to the highest standards. If any School employee is found to have breached this policy, they may be subject to the School disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

Complaints
Data Subjects who wish to complain to the School about how their personal information has been processed may lodge their complaint with the DPO.

If Data Subjects are not satisfied with the outcome of their complaint or the way in which it has been handled, they may also complain directly to the ICO.

Appendices:

Appendix 1: Privacy Notices
Appendix 2: Declaration of Consent for the Use of Staff Photographs at Agate Momentum Trust Schools

Appendix 1

Agate Momentum Trust
Privacy notices

Contents

……

1. Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.
This privacy notice explains how we collect, store and use personal data about **pupils**.
We, Agate Momentum Trust, are the 'data controller' for the purposes of data protection law.
Our data protection officer is NPW (Newham Partnership Working).

The personal data we hold
Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- Digital videos/ recording
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data
We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services and inform our planning to improve outcomes for pupils
- Administer admissions waiting lists

- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data
We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)
- The processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.
Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information
While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.
Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data
We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We retain records in line with the retention guidelines for schools recommended by the Information and Records Management Society: https://ico.org.uk/ / http://ldbsact.org/download/policies/Document%20Retention%20Schedule_Nov15.pdf

Data sharing
We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.
Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- 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.*

- 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.*
- 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.*
- Health and social welfare organisations- *to perform a public task in the public interests such as liaising with the schools dental service to promote good dental hygiene within our community*
- 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.*
- Police forces, courts, tribunals- *to perform a public task in the public interests, for example responding to and managing safe guarding concerns in order to keep our pupils safe within and beyond the school environment.*
- 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.*

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census and early years census.
Some of this information is then stored in the National Pupil Database (NPD https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information), which is owned and managed by the Department and provides evidence on school performance to inform research.
The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.
The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.
For more information, see the Department's webpage on how it collects and shares research data (https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data).
You can also contact the Department for Education (https://www.gov.uk/contact-dfe) with any further questions about the NPD.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.
Parents also have the right to make a subject access request with respect to any personal data the school holds about them.
If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request please contact our data protection officer at DPO@npw.uk.com

Parents/carers also have a legal right to access their child's **educational record**. To request access, please contact Hannah Cleland: School Business manager at:
hannah.cleland@scottwilkie.newham.sch.uk

Other rights
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer at DPO@npw.uk.com

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer DPO@npw.uk.com

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**: DPO@npw.uk.com

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

2. Privacy notice for pupils

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.
This privacy notice explains how we collect, store and use personal data about you.
We, Agate Momentum Trust, are the 'data controller' for the purposes of data protection law.
Our data protection officer is NPW (Newham Partnership Working).

The personal data we hold
We hold some personal information about you to make sure we can help you learn and look after you at school.
For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.
This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- Digital videos/ recording
- CCTV images

Why we use this data
We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing and to make plans to make the school better for you
- Look after your wellbeing

Our legal basis for using this data
We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.
Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information
While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.
We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data
We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.
We keep our records about you in line with the retention guidelines for schools recommended by the Information and Records Management Society: https://ico.org.uk/ / http://ldbsact.org/download/policies/Document%20Retention%20Schedule_Nov15.pdf

Data sharing
We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.
Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – *to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions in order to keep you safe and ensure that our school helps you to learn well.*
- The Department for Education– *to meet our legal obligations to share certain information with it, such as test outcomes so that we can compare ourselves against other schools and make sure that we are doing the best that we can to help you learn well.*
- 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 your progress to your parents so that together we can help you to achieve your best.*
- Suppliers and service providers – *to enable them to provide the service we have contracted them to do for example managing digital registers so that we know when you are in school and when you are away from school.*
- 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 make your learning even better.*
- 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.*
- Health and social welfare organisations- *to perform a public task in the public interests such as liaising with the schools dental service to promote good dental hygiene within our community*

- Professional advisers and consultants- *to perform a public task in the public interests in order, for instance, to evaluate how well we are doing, support and challenge school leaders and continue enabling you to do your best.*
- 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.*
- Police forces, courts, tribunals- *to perform a public task in the public interests, for example responding to and managing safe guarding concerns in order to keep you and your school friends safe within and beyond the school environment.*
- 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 help you to achieve your best.*

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.
Some of this information is then stored in the National Pupil Database (NPD https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information), which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.
The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.
The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.
For more information, see the Department's webpage on how it collects and shares research data (https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data).
You can also contact the Department for Education (https://www.gov.uk/contact-dfe) with any further questions about the NPD.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.
If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.
If you want to make a request please contact our data protection officer at DPO@npw.uk.com.

Your other rights over your data
You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints
We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.
You can make a complaint at any time by contacting our data protection at DPO@npw.uk.com
You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer: DPO@npw.uk.com

This notice is based on the Department for Education's model privacy notice for pupils, amended to reflect the way we use data in this school.

3. Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.
This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.
We, Agate Momentum Trust, are the 'data controller' for the purposes of data protection law.
Our data protection officer is NPW- Newham Partnership Working

The personal data we hold
We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data
The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data
We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.
Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information
While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.
Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data
We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.
Once your employment with us has ended, we will retain this file and delete the information in it in line with the retention guidelines for schools recommended by the Information and Records Management Society: https://ico.org.uk/ / http://ldbsact.org/download/policies/Document%20Retention%20Schedule_Nov15.pdf

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – *to meet our legal obligations to share certain information with it, such as in relation to safeguarding concerns with LADO.*
- The Department for Education- *to meet our legal obligations to share certain information with it, such as the annual school workforce census.*
- Your family or representatives- *to protect the vital interests of the data subject or another person in the case of a medical emergency for example.*
- Suppliers and service providers – *to enable them to provide the service we have contracted them for, such as NPW HR to issue employment contracts.*
- Financial organisations- *to enable them to provide the service we have contracted them for example to enable NPW to make salary payments into your account.*
- Central and local government- - *to meet our legal obligations to share certain information with it, such as the annual school workforce census.*
- Our auditors- *to perform a public task in the public interests for example to safe guard use of public funding.*
- Survey and research organisations- *to perform a public task in the public interests for example improving staff wellbeing through the charity Head start.*
- Trade unions and associations- *to perform a public task in the public interests for example performance management outcomes, disciplinary investigations.*
- Health authorities- *to perform a public task in the public interests ensuring that we manage our organisation effectively in promoting practice which supports employees in addressing health/medical needs.*
- Security organisations- *to enable them to provide the service we have contracted them to do for example CCTV and the digital sign in system.*
- Health and social welfare organisations- *to perform a public task in the public interests ensuring that we manage our organisation effectively in promoting practice which supports employees in addressing health/medical needs.*
- 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 for example improving staff wellbeing through the charity Head start.*
- Police forces, courts, tribunals- *to perform a public task in the public interests, for example responding to and managing safe guarding concerns in order to keep our pupils safe within and beyond the school environment.*
- Professional bodies- *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*
- Employment and recruitment agencies- *to meet our legal obligations to share certain information, such as providing references for employment.*

Transferring data internationally
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights
How to access personal information we hold about you
Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.
If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer at DPO@npw.uk.com

Complaints
We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113

- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**: DPO@npw.uk.com

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

Privacy Notice for Course Delegates

This privacy policy sets out how the Agate Momentum Trust uses and protects any information that you give us when you use the website, subscribe to our mailing list and participate in any of our course and projects.

The Agate Momentum Trust is committed to ensuring that your privacy is protected. Any information you provide us will only be used in accordance with this privacy statement.

What we collect
We may collect the following information:

- Name, Designation, CPD preferences
- Contact information including email address and telephone number
- School information such as postcode, URN and head teacher's email address
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Other information relevant to course and project evaluations

Our lawful basis for using this data

We only collect and use your personal data as permitted by law. Mostly, we process it where:

- we need to comply with a legal obligation
- we need it to perform an official task in the public interest
- we have obtained consent to use it in a certain way

Sometimes, we may also process your personal data in situations where:

- we need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use your personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent. If you wish to withdraw your consent then please email Hannah Cleland at hannah.cleland@scottwilkie.newham.sch.uk

Some of the reasons listed above for collecting and using your personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you, we will make it clear whether providing it is mandatory or optional. We will always tell you if it is optional.

What we do with the information we gather:
We require this information to understand your needs and provide you with a better service, and in particular for the following reasons:

- Internal record keeping and reporting to the DfE

- We may use the information to improve our programmes and services
- We may periodically send promotional emails about new projects, CPD programmes or other relevant information which we think you may find interesting using the email address which you have provided

How we store this data

We do not share information about you with any third party without consent unless the law and our policies allow us to do so. Where it is legally required or necessary (and it complies with Data Protection Law) we may share personal information about delegates with:

- Our Local Authority
- The Department for Education (a government department)
- Our regulator (the organisation or "watchdog" that supervises us), e.g. Ofsted
- Financial organisations – for course/service fees
- Central government
- Police forces, courts, tribunals

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)

- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer at DPO@npw.uk.com

Complaints
We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint, please contact our data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**: DPO@npw.uk.com

Security
We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.
In addition, we use this data, with your consent, to keep in touch with you on professional development opportunities and related matters. If you have any questions or concerns around our privacy policy please contact Hannah Cleland at hannah.cleland@scottwilkie.newham.sch.uk

If you would no longer like to receive Hallsville's Training School updates, please email Hannah and let us know.

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

Appendix 2

Declaration of Consent for the Use of Staff Photographs at Agate Momentum Trust Schools

Agate Momentum Trust is committed to respecting your privacy and takes privacy matters seriously.
The company would like to use your name and photograph and the name of the school you work in for security passes. The legal basis for utilising this information is to perform a public task in the public interests in relation to managing safe guarding, in order to keep our pupils and staff safe within the school environment.

There may also be occasions when the Agate Momentum Trust would like to use your photograph in sales and marketing materials including the Trust and school websites and other social media platforms. Your consent will be the legal basis for utilising this personal information. You can choose to consent to the use of your photograph being on display and being shown on internal emails and for sales and marketing material, separately.

Agate Momentum Trust operates on a membership basis. In order to provide a personal service for students and their families which connects with the educational outcomes we are trying to achieve, we feel that the use of photographs helps to strengthen relationships.

You can also in future choose to withdraw your consent at any time by contacting Hannah Cleland. (Details will be removed within 10 working days)

This information will not be shared with any other party nor will it be used for any other purpose without your explicit consent.

The information will be displayed and retained for the duration of your employment with Agate Momentum Trust.

I consent that my photograph can be used to celebrate and share success on the school website and the school's twitter feed.

Yes ☐
No ☐

I consent that my photograph can be used on internal emails

Yes ☐
No ☐

I consent that my photograph can be used in sales and marketing materials related to Agate Momentum Trust

Yes ☐
No ☐