Ashgate Specialist Support Primary School
Crossacres Rd, Wythenshawe, M22 5DR
Tel:0161 359 5322 Fax: 0161 437 8601
email: admin@ashgate.manchester.sch.uk
Headteacher: Diane Wolstenholme B.Ed.Hons

POLICY STATEMENT:

Data Protection Policy

UN Convention on the Rights of the Child

Article 3 (best interests of the child) The best interests of the child must be a top priority in all decisions and actions that affect children.
Article 13 (freedom of expression) Every child must be free to express their thoughts and opinions and to access all kinds of information, as long as it is within the law.
Article 16 (right to privacy) Every child has the right to privacy. The law should protect the child's private, family and home life, including protecting children from unlawful attacks that harm their reputation.
Article 23 (children with a disability) A child with a disability has the right to live a full and decent life with dignity and, as far as possible, independence and to play an active part in the community. Governments must do all they can to support disabled children and their families.

Date policy written	December 2019
Reviewed Consultation and Ratified	
Review date	

Contents:

1. Introduction

1.1 Ashgate Primary School strives to provide the best possible education for our pupils. It aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

2.1 Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. It reflects the ICO's code of practice for the use of surveillance cameras and personal information. The ICO is the UK's independent regulator responsible for upholding and enforcing the rights of individuals under data protection law. The School is registered with the ICO, as legally required. Our registration number is Z9474900.

3. Definition

TERM	DEFINITION
Personal data	Any information relating to an identified or identifiable living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing personal data. Data controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Data Protection Act.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

Our School processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

5. Scope

5.1 This policy applies to all of the School's personal data in relation to pupils, staff, governors, suppliers and any other personal data the school processes from any source. It should be read in conjunction with other relevant school policies such as the eSafety policy.

6. Roles and responsibilities

6.1 This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. This policy and procedures explain the duties and responsibilities placed on the school under the legislation relating to data protection issues to ensure that all data is handled and stored securely.

6.2 Governance

The Board of Governors and the Headteacher are committed to compliance with all relevant UK and EU data protection legislation in respect of personal data, and the protection of the rights and freedoms of individuals whose information the School collects and processes.

6.3 The Data Protection Officer

The School has appointed a Data Protection Officer (DPO) who will assist the school in monitoring its compliance with the legislation. The responsibilities of the Data Protection Officer will include the following:

- Keep the Board of Governors and Senior Management updated about data protection responsibilities, risks and issues;
- Act as an advocate for data protection within the School;
- Monitor compliance with EU Regulations on data protection, ePrivacy and UK Data

- Protection Laws and Regulations;
- Monitor the data protection policy, ensuring it is reviewed and updated on a regular basis;
- Ensure that the School provides appropriate data protection training and advice for all staff members and those included in this policy;
- Provide advice where requested as regards the data protection impact assessments and monitoring that such assessments are completed to an appropriate standard;
- Provide advice on data protection matters for staff, governors, parents and other stakeholders;
- Respond to individuals such as parents and employees who wish to know which data is being held on them by the School;
- Ensure that appropriate data processing agreements are put in place with third parties that handle the School's data and ensure that reviews are carried out of third parties on a regular basis;
- Ensure that the record of data processing is updated regularly;
- Act as a contact point and provide cooperation with the Office of the Information Commissioner.

6.4 All staff

Staff are responsible for:

• Collecting, storing and processing any personal data in accordance with this policy

• Informing the School of any changes to their personal data, such as a change of address

• Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not, they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

7 Data Protection Act 2018

7.1 From 25 May 2018, the General Data Protection Regulation (GDPR) as supplemented by the UK Data Protection Act 2018 took legal effect. This replacement data protection framework places new obligations on organisations and strengthens the rights that individuals have over the processing of their personal information.

7.2 These rights of the individuals are as follows;

- the right to be informed;
- to ask us for access to copies of the personal information we hold about you;
- to ask us to rectify your personal information if it is inaccurate or incomplete;
- to ask us to stop processing your personal information (this is known as the 'right to object');
- to ask us to erase personal information we hold about you (this is also known as the 'right to be forgotten');
- to ask us to 'restrict' the processing of your personal information (e.g. restrict our access and use pending our consideration, for example, of any objection or erasure request you have submitted);
- to ask us to ensure that a decision which legally affects you is reviewed by a person if the decision has been made solely using an automated computerised process;

- to ask us to put the personal information you have given us into a portable electronic machine readable format so it is capable of being transmitted to someone else.

7.3 Please be aware that these rights are not absolute and are subject to conditions and exemptions. In some cases the rights described above only apply if the processing activity is undertaken on specific legal grounds and/or in defined circumstances. Therefore all of these rights are unlikely to be engaged in all cases. Full information about individual's rights can be found on the ICO website.

7.4 Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

7.5 The Data Protection Act 2018 is underpinned by important principles. School's policies and procedures are designed to ensure compliance with the following principles:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside of the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

8 Collecting personal data

8.1 Lawfulness, fairness and transparency

- We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:
    - The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
    - The data needs to be processed so that the school can **comply with a legal obligation**
    - The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life
    - The data needs to be processed so that the school, as a public authority, can **perform a task in the public interest or exercise its official authority**
    - The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
    - The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

8.2 For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

• The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

• The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**

• The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent

• The data has already been made **manifestly public** by the individual

• The data needs to be processed for the establishment, exercise or defence of **legal claims**

• The data needs to be processed for reasons of **substantial public interest** as defined in legislation
• The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
• The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
• The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

8.3 For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.
- We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

9 Limitation, minimisation and accuracy

9.1 We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

- If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.
- Staff must only process personal data where it is necessary in order to do their jobs.
- We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the trust's record retention schedule.

10 Sharing personal data

10.1 We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

• There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
• We need to liaise with other agencies. We will seek consent as necessary before doing this
• 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 contract with the supplier or contractor 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
- We will also share personal data with law enforcement and government bodies where we are legally required to do so.
- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.
- Where we transfer personal data internationally, we will do so in accordance with data protection law.
- To comply with the Data Protection Act the school must:
- Manage and process personal data properly
- Protect the individuals' right to privacy
- Provide an individual with access to all personal data held on them.

11. Subject access requests and other rights of individuals

11.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- he right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO or a member of the Senior Leadership Team.

11.2 Children and subject access requests

- Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

11.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification

- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

12 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

13 CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.
We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to our Data Protection Officer, who is contactable via schools.dpo@manchester.gov.uk

14 Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers, for photographs and videos to be taken of pupils for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.
Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Our esaftey policy states that any photographs or video footage stored must be deleted immediately once no longer needed. Class teachers are responsible for collating key photos of each child in a folder at the end of the academic year. This folder is transferred to the child's next teacher and any unwanted photos will be deleted. When the pupil reaches the end of Year 6, their folder of photographs is archived by Infinity Computing and stored for 8 years before being deleted.

15 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply

Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure.

16 Data security and storage of records

We will 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 hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites

Encryption software is used to protect all portable devices and removable media, such as laptops.
Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy/acceptable use agreement)
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.

17 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18 Personal data breaches

- The School will make all reasonable endeavours to ensure that there are no personal data breaches.
- In the unlikely event of a suspected data breach, we will report the data breach to the ICO within 72 hours after becoming aware of it, where this is required by law. Such breaches in a school context may include, but are not limited to:
  - Safeguarding information being made available to an unauthorised person
  - The theft of a school laptop containing non-encrypted personal data about pupils

19 Training

All staff will receive training on this policy. New members of staff will receive compulsory training as part of the induction process. Training will be refreshed yearly or whenever there is a substantial change in the law or the School's policy and procedures.
Training will cover:

- The General Data Protection Regulation and its impact on schools;
- School's data protection management and related policies and procedures.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

- This policy will be reviewed every **2 years** and shared with the full governing board.

21. Links with other policies

- eSafety
- Child Protection Policy

22. Where to go if you have queries about the data protection policy

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk
Additional Information below from the ICO website
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
If you have queries on any aspect of this policy, or the GDPR in general, please contact the School's Data Protection Officer:
Tom Powell, Head of Internal Audit, Manchester City Council
schools.dpo@manchester.gov.uk
0161 600 7993