Aintree Davenhill Primary School

Data Protection Policy

Approved by the Headteacher

Review Date: July 2026

Aims

Aintree Davenhill Primary School is required to keep certain personal data about its staff and pupils in order to fulfil its purpose and to meet its legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

Our school 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 (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.
All members of staff at Aintree Davenhill Primary School have been provided with Data Protection and GDPR awareness training and will receive annual refresher training alongside any training/information updates as and when deemed appropriate to ensure the ongoing best practice in data protection in the school. The policy is communicated to all staff and they are expected to understand and abide by it. Any breach of this policy will be taken seriously and may result in formal action being taken.
Any member of staff, pupil, parent, governor or visitor who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Protection Lead, Mrs Nicky Williams or the Data Protection Officer, Mr Peter Rafferty. External stakeholders have access to this policy via the school website.

Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access request.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

Definitions

Personal Data

Any information relating to an identified, or identifiable 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
- 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 of personal data.

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.

The Data Controller
Aintree Davenhill Primary School processes personal data relating to parents, pupils, staff, governors, visitors and others, and is, therefore, a data controller and responsible for implementation. As a Data Controller, the school must 'notify' (register with) the Information Commissioner's Office (ICO) under the GDPR annually. Aintree Davenhill Primary School is registered with the ICO under reference Z7386600.

If you have any questions regarding Data Protection at Aintree Davenhill Primary School, please contact the Data Protection Lead, Mrs Williams on 0151 526 1162 or email finance.aintreeedavenhill@schools.sefton.gov.uk . Alternatively, you may contact the Data Protection Officer, Mr Peter Rafferty by email on raff31@gmail.com

Roles and Responsibilities
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.

Governing Body
The School is a registered Data Controller and Governors hold overall responsibility to ensure that our school complies with all relevant data protection obligations and that:

- the policy is reviewed every year.
- the policy is clearly communicated, implemented and monitored by the school.

Data Protection Officer
The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide a report of their activities to the Governing Body and, where relevant, report to the Governing Body their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Our DPO is Mr Peter Rafferty and is contactable via school on 0151 526 1162 or by email raff31@gmail.com.

Headteacher
The Headteacher will ensure that:

- the policy reflects up to date best practice in data management, security and control

- the policy is clearly communicated to all stakeholders and the school's obligations under the policy are fully met
- the school complies fully with the GDPR and manages its information and records appropriately.

Data Protection Lead (DPL)
The Headteacher has designated a single point of contact for all matters relating to data protection in Aintree Davenhill Primary School known as the Data Protection Lead (DPL). This role is held by the School Business Manager. The DPL will ensure that:

- the school complies fully with the GDPR and manages its information and records appropriately
- the school provides clear communication to stakeholders about what/why personal data is collected and details of any sharing of information. The school will do this via 'Privacy Notices' which will be issued to stakeholders
- all staff who are responsible for handling personal data are fully aware of, and understand, the school's obligations and receive the appropriate training
- the school registers with the Information Commissioner's Office (ICO) annually
- the school shares information with others only when it is legally appropriate to do so or where explicit consent has been received by the data subject
- personal information is not retained for longer than is necessary and that when obsolete information is destroyed, it is done so appropriately and securely
- procedures are in place to ensure compliance with the duty to respond to requests for access to personal information, known as 'Subject Access Requests' (SAR)
- all necessary precautions are in place to protect against physical loss or damage, and that both access and disclosure is restricted, irrespective of the format in which it is recorded.

All Staff
Data Protection is a responsibility of all staff at Aintree Davenhill Primary. All 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 DPL/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.

<u>Data Protection Principles</u>
The GDPR is based on compliance with the following data protection principles requiring that data is:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary for the purposes for which it is processed
- processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

Collecting Personal Data

Lawfulness, Fairness and Transparency

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

1. 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
2. the data needs to be processed so that the school can comply with a legal obligation
3. the data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
4. the data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
5. the data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
6. the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

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

If we offer online services to pupils, such as classroom apps, we will get parental consent.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, Minimisation and Accuracy

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.
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 school's Record Management procedures.

Sharing Personal Data

We will not normally share personal data with anyone else, but may do so 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 data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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

- the prevention or detection of crime and/or fraud

- the apprehension or prosecution of offenders
- the assessment or collection of tax owed to HMRC
- in connection with legal proceedings
- where the disclosure is required to satisfy our safeguarding obligations
- research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

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 students or staff.
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.

Subject Access Requests (SAR) and other Rights of Individuals

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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
- 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.

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

- name of individual
- correspondence address
- contact number and email address
- details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO or DPL.

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. Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request.

Responding to Subject Access Requests

When responding to requests, we:

- may ask the individual to provide two forms of identification
- may contact the individual via phone to confirm the request was made
- will respond within one month of receipt of the request
- will provide the information free of charge unless the request is substantial and/or complicated

- may tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

We will or may not disclose information if:

- it might cause serious harm to the physical or mental health of the pupil or another individual
- it would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests (Safeguarding)
- it is contained in adoption or parental order records
- it is given to a court in proceedings concerning a child
- the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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 (see section 7), 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, or object to the processing of it (in certain circumstances)
- prevent use of their personal data for direct marketing
- challenge processing which has been justified on the basis of public interest
- request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- 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.

Parental Requests to See the Educational Record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a student) within fifteen school days of receipt of a written request.

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. The CCTV system is in operation to detect and prevent crime and improve safety.

Any enquiries about the CCTV system should be directed to the Headteacher, School Business Manager or Premises staff.

Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals in 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. Uses may include:

- in school on notice boards and in newsletters, etc.
- outside of school by external agencies such as the school photographer, newspapers
- online on our school website or Facebook page.

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 only use the forename of the student.

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 privacy 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
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

<u>Data Security and Storage of Records</u>
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 are kept securely stored when not in use
- papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access, with the exception of essential medical information.
- where personal information needs to be taken off site, staff must protect the information in the same manner they would do if in school
- a strong password policy is in place to protect access to school hardware and IT infrastructure. Staff and pupils are reminded to change their passwords at regular intervals.
- encryption software is used to protect portable devices and removable media, such as USB devices

- staff, students 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 ICT Acceptable Use Policies and Online Safety Policy)
- 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.

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 an accredited 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.

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 follow the procedure set out in Appendix 1. All data breaches will be recorded and shared with our DPO who will advise on further reporting required to the ICO.

Training

All staff and Governors are provided with data protection guidance as part of their induction process. Data protection will also form part of continuing professional development where changes to legislation, guidance or the school's processes make it necessary.

Monitoring Arrangements

This policy will be reviewed annually by the school and presented to the Governing Body for approval.

Links with Other Policies

This policy should be read in conjunction with the following school policies:

- Safeguarding Policy
- Privacy Notices
- E-Safety Policy
- ICT Acceptable Use Policy (Staff)
- Records Management procedures

Appendix 1: Personal Data Breach Procedure
This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - lost
  - stolen
  - destroyed
  - altered
  - disclosed or made available where it should not have been
  - made available to unauthorised people.
- The DPL will alert the Headteacher and the Chair of Governors
- The DPO & DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. Actions relevant to specific data types are set out at the end of this procedure
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage e.g. emotional distress by:
  - loss of control over their data
  - discrimination
  - identify theft or fraud
  - financial loss
  - unauthorised reversal of pseudonymisation
  - damage to reputation
  - loss of confidentiality
  - any other significant economic or social disadvantage to the individual(s) concerned.
- If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the School's computer system.
- Where the ICO must be notified, the DPO will do this via the report a breach page of the ICO website within 72 hours. As required, the DPO will:
  - set out a description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned.
  - the name and contact details of the DPO
  - a description of the likely consequences of the personal data breach
  - a description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours.
The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- the name and contact details of the DPO
- a description of the likely consequences of the personal data breach
- a description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- facts and cause
- effects
- action taken to contain it and ensure it does not happen again such as establishing more robust processes or providing further training for individuals.

Records of all breaches will be stored on the school's computer system. The DPO, DPL and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Sensitive information being disclosed via email (including safeguarding records)
If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error. Members of staff who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the ICT department to recall it. In any cases where the recall is unsuccessful, the DPL will contact the DPO and relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request. The DPO will carry out an internet search to check that the information has not been made public; if it has; we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.