Data Protection Policy

for

The ACE Centre Nursery School

This policy was adopted by a meeting of The ACE Centre Nursery School governors:

Date to be reviewed: April 2025

Signed: Catherine Hayward **(Chair of Governors)**

Signed: Lynn Jenkins **(Headteacher)**

Introduction

The ACE Centre Nursery collects and uses personal information about staff, pupils and other individuals who come into contact with the School. This information is gathered to enable provision of care, education and other associated functions. In addition there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

Schools have a duty to be registered as Data Controllers with the Information Commissioner's office (ICO) detailing both information held and its use. These details are available on the ICO's website. Schools also have a duty to issue a privacy notice to all parents. This summarises the information held, why it is held and the other parties to whom data may be passed on to.

Purpose

This policy is intended to ensure that all personal information relating to staff, children, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation 2016 (GDPR) and Data Protection Act 2018 (DPA).

It is applied to all information regardless of how it is collected, used, recorded, stored and destroyed, irrespective o whether this is stored in paper files or electronically.

All staff involved in the collection, processing and disclosure of personal data will be aware of their duties and responsibilities through adherence to these guidelines.

This policy meets the requirements of the GDPR and DPA, which is based on guidance published by the Information Commissioners Office (ICO). It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record

Roles and Responsibilities

This policy applies to all staff employed by The ACE Centre Nursery and to all organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Governing Body:	The governing body has overall responsibility for ensuring compliance with relevant data protection obligations.
Data Protection Officer:	The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law and developing related policies and guidelines. The DPO is the first point of contact for individuals whose data is processed and the ICO. Our DPO is Rob Horsfall.
Headteacher:	The headteacher acts as the representative of the data controller on a day-to-day basis.

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 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 (EEA)
    - 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

Data Protection Principles

The GDPR is based on data protection principles that school must comply with, which dictate that personal data must be:

- 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

Personal information or data is information that relates to a living individual, who can be identified from that data, or from that data together with other information available to them.

Personal data includes (but is not limited to) an individual's name, address date of birth, photograph, bank details or other information that identifies them.

Sensitive personal data includes information relating to an individual's criminal record, ethnicity or racial origin, physical or mental health or disability, political opinions, religious beliefs or beliefs of a similar nature, sexual orientation or trade union affiliation.

Collecting and Processing Personal Data

Lawfulness, Fairness and Transparency

Personal data will only be processed where there is one of six 'lawful bases' 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, providing the individual's rights and freedoms are not overridden
- The individual (or their carer/parent when appropriate in the case of a pupil) has freely given clear consent

Sensitive personal data will only be processed if one of the special category conditions for processing under data protection law has been adhered to:

- The individual (or their carer/parent 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 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

Processing of data relating to criminal offences will require both a lawful basis and condition stipulated within data protection law, these conditions include:

- The individual (or their carer/parent 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

In the first instance when personal data is collected directly from an individual, they will be provided with relevant information required by data protection law. When processing data fairness will always be considered, ensuring that personal data is not handled in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

Limitation and Accuracy

Personal data will only be collected for specified, explicit and legitimate reasons, explained to individuals when first collected. If this personal data is to be used for other reasons than those explained when first collected, individuals will be informed in the first instance and consent obtained where necessary.

Personal data must only be processed by staff where it is necessary to support role completion. Data will be kept accurate and up-to-date, inaccurate data will be rectified or erased as appropriate.

When personal data is no longer required by staff it must be deleted or anonymised and archived in accordance with record retention guidance.

Sharing Personal Data

Although personal data is not normally shared without consent there are certain circumstances where it may be necessary to do so. These include (but are not limited to) situations where:

- There is an issue with a pupil or carer/parent that puts the safety of our staff at risk
- Liaison with other agencies is required (consent will be sought)
- Suppliers or contractors need data to enable provision of service to our staff and pupils (e.g. ICT companies). However:
    - Only suppliers or contractors will be appointed that can guarantee compliance with data protection law
    - A contact will be established with the supplier or contractor to ensure the fair, lawful processing of any personal data shared
    - Data will only be shared that the supplier or contractor needs to carry out their service

If legally required to do so the school will share personal data with law enforcement and government bodies. Personal data may also be shared with emergency services and local authorities to support an emergency situation effecting any pupils or staff.

If personal data is transferred internationally this will be done in accordance with data protection law

Subject Access Requests

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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The 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, however, to support timely response these should be 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 be forward to the DPO.

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's carers or parents. For a carer or parent 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 below the age of twelve are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from carers or parents of pupils at school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, school will:

- Ask the individual to provide two forms of identification
- Contact the individual via phone to confirm the request
- Respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Provide the information free of charge
- Inform the individual we will comply within three months of receipt of the request, where a request is complex or numerous. The individual will be informed of this within one month, providing an explanation of why the extension is necessary

In number of circumstances information may not be disclosed, 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 or confidential references

A request may be refused in it is unfounded or excessive, or a reasonable administration fee may be charged. When making this decision consideration will be given to the request being repetitive in nature. If a request is refused the reasoning will be communicated to the individual and they will be informed of their right to complain to the ICO or seek to enforce their subject access right through court order.

Educational Record – Parental Requests

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 pupil) within fifteen school days of receipt of a written request.

An administration fee may be charged if the request is for a copy of the educational record.

This right applies as long as the pupil concerned is aged under 18. There are certain circumstances in which this right can be denied, e.g. releasing the information might cause serious harm to the physical or mental health of the pupil or another individual.

Individual Data Protection Rights

In addition to the right to make a subject access request and to receive information when data is being collected, used and processed individuals also have the right to:

- Withdraw their consent to processing at any time
- Request rectification, erasure or restricted 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
- Request 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.

CCTV

The school has a number of CCTV cameras in various locations on the premises to support safety, security and safeguarding. The ICO's code of practice for the use of CCTV will therefore be adhered to.

It is not required to obtain individuals' permission to use CCTV, however it is made clear that individuals are being recorded. Security cameras are clearly visible and signage indicates that CCTV is in use.

Any enquiries relating to the CCTV system should be directed to the DPO.

Photographs and Videos

As part of school activities, photographs may be taken, or videos recorded of individuals within the premises.

Written consent must be obtained from carers/parents for photographs and videos to be taken of their child for communication, developmental, marketing and promotional materials. The intended use of these photographs and/or videos should be clearly explained to both the carer/parent and child. Any photographs and videos taken by carers/parents 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 carers/parents have agreed.

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 or publication
- Online on our school website or social media pages
- On our reception presentation

Consent can be refused or withdrawn at any time. If consent is withdrawn, all associated photographs or videos must be deleted and distribution ceased.

Photographs and videos used in this manner must not be accompanied by any other personal information about the child, ensuring that they cannot be identified.

Data Protection by Design and Default

Measures will be implemented to ensure that data protection has been integrated into all data processing activities, including:

- Appointing a suitably qualified DPO, ensuring they have the necessary resources to fulfil these duties, maintaining 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
- 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 privacy measures, ensuring compliance
- Implementation of appropriate safeguards if any personal data is transferred outside the EEA
- Maintaining records of all processing activities, including:
    - For the benefit of data subjects: Making available the name and contact details of school and DPO and all information we are required to share about how we use and process their personal data (via 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 the data is being used, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how data security is maintained

Data Security and Record Storage

All personal data must be protected and safeguarded from:

- Unauthorised or unlawful access, alteration, processing or disclosure
- Accidental or unlawful loss, destruction or damage

As such:

- Paper based records and portable electronic devices, such as laptops and hard drives containing personal data, must be stored securely when not in use e.g. in a locked cabinet or office
- Papers containing confidential personal data must not be left on office and classroom desks, staffroom tables, or indeed anywhere where there may be unrestricted access
- Where personal information needs to be taken off site, staff must sign it in and out from reception
- Passwords used to access school computers, laptops and other electronic devices must be secure, containing letters and numbers. Staff are reminded that they should not reuse passwords from other sites
- Encryption is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or governors that store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where personal data is shared with a third party due diligence must be undertaken and processes followed to ensure security and protection

Record Disposal

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, if it does not need to be, or cannot be rectified or updated.

All paper-based records will be shredded or incinerated, and electronic files deleted, in accordance with appropriate retention periods. If third parties are used to safely dispose of records on the school's behalf, sufficient guarantee of compliance to data protection law must be sought.

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, the Personal Data Breech Procedure will be implemented by the DPO.

When appropriate, the data breach will be reported to the ICO within 72 hours after becoming aware of it.

Such breaches in a school context may include (but are not limited to):

- A non-anonymised dataset being published on the school website which shows names of pupils eligible for pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils