Data Protection Policy

Introduction

This policy outlines The Acorn Nursery School's commitment to protect the privacy of children, parents, staff, and others, in line with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Scope

This policy applies to all staff, volunteers, and third parties who handle, store, or process personal data on behalf of the nursery.

Definitions

Personal data	Any information that relates to an identifiable person who can be directly or indirectly identified from the information, for example, a person's name or date of birth.
Special categories of personal data	Any data which relates to an individual's health, race, ethnic origin, political opinion, religion, trade union membership, genetics and sexual orientation.
Data Processing	Anything done to personal data such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.
Data Controller	A person or organisation that determines the purposes and the means of processing data.
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

The Acorn Nursery School processes data relating to children, parents, staff, and others, and therefore is a data controller. The Acorn Nursery School are registered as a data controller with the Information Commissioner's Office (ICO) and will renew this registration annually or as legally required.

Roles and responsibilities

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. The DPO is the first point of contact for individuals whose data the nursery processes. Our DPO is Wendy Hastie, Nursery Manager.

All Staff

Staff are responsible for collecting, storing and processing any personal data in accordance with this policy.

Principles

The Acorn Nursery School commits to:

- Processing personal data lawfully, fairly, and transparently.
- Collecting data for specific and legitimate purposes.
- Ensuring data is relevant, accurate and up to date.
- Retaining data for no longer than necessary.
- Keeping data secure against unauthorised access or loss.

Data Collection
We will:

- Obtain explicit consent before collecting personal data.
- Inform individuals of the reasons for collecting their data.
- Collect only the data necessary for our operational needs.

We use this data to:

- Support children's learning.
- Makes assessments on children's development.
- Safeguard the children in our care in accordance with relevant legislation.
- Comply with Government legislation.
- Assess the quality of our services.

The Acorn Nursery School collect, hold and share two kinds or records on children attending our setting:

Developmental records
These include:

- Developmental information collected prior to the child starting at the setting.
- The child's Two Year Progress Check (saved on Tapestry and shared with parents).
- Observations of children, photographs, video clips are shared with parents via Tapestry.

Personal records
These include:

- Personal details – including the information provided on the child's registration form and any consent forms and characteristics such as ethnicity, language and nationality.
- Contractual matters – including the child's days and times of attendance, a record of the child's fees and/or funding entitlement, any records of fee reminders and/or disputes.
- Emergency contact details – including those people, other than parents/guardians with authorisation to collect the child from the setting.
- Children's health and well-being – including discussions about every day matters regarding the health and well-being of the child with the parent/guardian, records of accidents and medication records.
- Safeguarding and child protection concerns – including records of all welfare and protection concerns and our resulting actions, meetings and telephone conversations about the child and any information regarding a Looked After Child.
- Early support and SEN – including any focussed intervention provided by our setting, a record of the child's SSP and, where relevant, their EHCP.
- Correspondence and reports – including letters and emails to and from other agencies and any confidential reports relating to specific children.

Data Security
The Acorn Nursery School implement technical and organisational measure to ensure data is secure, including:

- Access to children's files is restricted to those authorised to see them such as the Head of Nursery, Manager, Deputy Manager, the Designated Safeguarding Lead (DSL), the Deputy DSL, the child's key person and, if relevant the nursery SENDCo.
- Physical files are stored in a cupboard which is locked at the end of the nursery day.
- Password protection and encryption is used for electronic data.

- Staff who store personal information on their personal devices are expected to follow the same security procedures as for nursery owned equipment.
- 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.

Staff can be held personally liable in law under the terms of the Data Protection Act. They may also be subject to claims for damages from persons who believe they have been harmed as a result of inaccuracy, unauthorised use of disclosure of the data. A deliberate breach of the Data Protection Policy will be treated as a disciplinary matter and serious breaches could lead to dismissal.

Disposal of Records

Personal data that is no longer needed will be disposed of securely. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files.

Types of Records and Retention Periods:

Type of Record	***Retention period***	***Legislation***
Registration forms	3 years after the child leaves the setting	EYFS 2025 ICO 2018
Attendance registers	3 years after the child leaves the setting	EYFS 2025 ICO 2018
Local Authority funding documents	7 years (plus the current financial year)	Local Authority Funding Contract
Medication forms	3 years after the child leaves the setting	EYFS 2025 ICO 2018
Minor accident and incident forms	3 years after the child leaves the setting	EYFS 2025 ICO 2018
Serious accident and incident forms	Until the child reaches the age of 21 years	Limitation Act 1980
Child protection files	Until the child reaches the age of 21 years old; 75 years for Looked After Children OR handed to the child's next setting when the child leaves or moves to school	Limitation Act 1980 Surrey Safeguarding Children Partnership
Special Educational Needs and Disability (SEND) records	Until the child reaches the age of 25 years	Limitation Act 1980
Complaints records	3 years	EYFS 2025
Non-statutory records including Tapestry profile	Transferred to parents when the child leaves the setting	ICO 2018
Children's photos including those used on the Acorn Nursery School website	Until no longer useful for the purpose for which they were taken or if parental permission is withdrawn	ICO 2018

Data Sharing

The information that you provide to us, whether mandatory or voluntary, will be regarded as confidential. We do not share information about your child with anyone without consent unless the law and our policies allow us to do so.

We routinely share information without consent with:

- Schools that children attend after leaving us.
- Our local authority for the purposes of FEE and the Early Years Census.
- The Department for Education (DfE) as part of statutory data collections.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including 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 pupils or staff.

Subject Access Requests

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

Children's developmental records are shared regularly with parents / guardians via Tapestry and formal requests to access these is not required.

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

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

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 below the age of 12 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 parents or carers of pupils at our nursery 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, 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.
- Will provide the information free of charge.
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual.
- 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.
- Is contained in adoption or parental order records.

- Is given to a court in proceedings concerning the child.

If a 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, 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, 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.
- 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.

Data Breach

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Where a data breach has taken place, staff need to complete the Data Breach form in Appendix 2.

Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a nursery tablet containing non-encrypted personal data about pupils

Staff Training

All staff will receive training on data protection principles, policy, and procedures. They are expected to uphold these principles in their roles.

Review

This policy will be reviewed annually, or more frequently if required by changes in data protection legislation.

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 complete the form in Appendix 2 and send to the Head of Nursery who will then 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 DPO 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 work out 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), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it's 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 securely electronically by the Head of Nursery.
- 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
        - 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 securely on the nursery computer system.
- The DPO and Head of Nursery will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

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 DPO as soon as they become aware of the error.
- In any cases where the recall is unsuccessful, the DPO will contact the 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.
- A nursery tablet containing non-encrypted sensitive personal data being stolen or hacked.

Appendix 2: Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please complete the form below and give to Head of Nursery immediately, complete Section 1 of this form

Section 1: Notification of Data Security Breach	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	