Data Protection and Cyber Security Policy

Introduction

Archfield House Nursery Ltd. takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

What is contained within this policy?

- Key principles
- Data protection principles
- How we define personal data
- How we define special categories of personal data
- How we define processing
- How will we process your personal data
- Special categories
- Sharing your personal data
- How should you process personal data for the company
- How to deal with data breaches
- Subject access requests
- Your data subject access rights

Key principles

This policy applies to current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

We have separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. We also have measures in place to protect the security of your data in accordance with our Data Security Policy. We will hold data in accordance with our Data Retention Policy. A copy of the documents mentioned in the above paragraphs can be obtained upon request from Rebecca Clevett, Nursery Director.

We will only hold data for as long as necessary for the purposes for which we collected it.

Archfield House Nursery Ltd. is a 'data controller' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, Archfield House Nursery Ltd.

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, we intend to comply with the 2018 Act and the GDPR.

Data protection principles
Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data
'Personal data' means information which relates to a living person who can be identified from that data (a 'data subject') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;

- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;
- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured on CCTV, by photograph or video);
- DBS (Disclosure and Barring Service)
- any other category of personal data which we may notify you of from time to time.

How we define special categories of personal data
'Special categories of personal data' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

How we define processing
'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data
Archfield House Nursery Ltd. will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

Examples of when we might process your personal data

We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

For example see below. For the meaning of the asterisks see Special categories):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;
- to monitor diversity and equal opportunities*;
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others;
- to monitor and protect the health and safety of you, our other staff, customers and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- to pay trade union subscriptions*;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;

- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- for any other reason which we may notify you of from time to time.

We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting Rebecca Clevett.

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims;
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

Personal data relating to criminal convictions and offences can be processed only:

- when it is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects.

Special categories
We might process special categories of your personal data for the purposes which have an asterisk (*) beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

We do not take automated decisions about you using your personal data or use profiling in relation to you.

Sharing your personal data
Sometimes we might share your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests. Information on this can be can be found in the Applicant or

Employee Privacy notice or by contacting the Data Protection Officer, Rebecca Clevett.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

How should you process personal data for the company
Everyone who works for, or on behalf of, Archfield House Nursery Ltd. has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security and Data Retention policies.

The Data Protection Officer, Rebecca Clevett is responsible for reviewing this policy and updating the Directors on the their data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

- You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords.
- You should lock your computer screens when not at your desk.
- Personal data should be encrypted/password protected before being transferred electronically to authorised external contacts.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer, Rebecca Clevett.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.
- Personal data should be shredded and disposed of securely when you have finished with it.

- You should ask for help from our Data Protection Officer, Rebecca Clevett if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact Rebecca Clevett immediately and keep any evidence you have in relation to the breach.

Subject access requests

Data subjects can make a 'subject access request' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer, Rebecca Clevett who will coordinate a response.

If you would like to make a SAR in relation to your own personal data you should make this in writing to Rebecca Clevett. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

Your data subject rights

You have the right to information about what personal data we process, how and on what basis as set out in this policy.

- You have the right to access your own personal data by way of a subject access request (see above).
- You can correct any inaccuracies in your personal data. To do you should contact Rebecca Clevett.
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Rebecca Clevett.

While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Rebecca Clevett.

- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- You have the right to be notified of a data security breach concerning your personal data.

In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Rebecca Clevett.

You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Cybersecurity

Purpose and Scope

- **Purpose**: To protect sensitive information about children, families, and staff; to safeguard the nursery's IT systems; and to reduce risk of cyber incidents (data breaches, malware, phishing) in line with the NCSC guidance. (NCSC)
- **Scope**: This policy applies to all staff, contractors, volunteers, and anyone with access to nursery data or IT systems (computers, tablets, smartphones, cloud services).

2. Governance and Responsibilities

Rebecca Clevett is our Designated Cyber Security Security Lead, they are responsible for overseeing cyber security, implementing this policy, and coordinating response to incidents. https://www.ncsc.gov.uk/guidance/early-years-practitioners-using-cyber-security-to-protect-your-settings

All staff must follow this policy, complete cyber security awareness training, and report any concerns or incident to the Cyber Security Lead.

Key Principles

This policy is based on the NCSC's "four steps" for early years settings: back up data, use strong passwords, protect devices, and deal with suspicious messages.

Backups

We maintain regular backups external hard drives or cloud storage across the devices of the nursery and periodically test recovery from backups to ensure data can restored reliably.

Passwords and Access Control

All nursery devices have password protection and we use strong, unique passwords, avoiding simple or predictable passwords (e.g., birthdays, pet names).

Our emails use multi-factor authentication (MFA) for access.

Our data management means there is limited access to sensitive data i.e. separate ‘dropboxes’.

We use online password generators to create secure passwords. Passwords will be changed at least annually.

Passwords will be stored on encrypted devices on a password protected document and passwords for these documents will be regularly changed.

Device Protection

We use antivirus / anti-malware software on nursery computers and laptops and update this software regularly, when prompted. We ensure systems, apps and firmware stay up to date by regularly install security updates.

All portable devices (tablets and laptops) are encrypted, locked when not in use, and physically stored securely at the end of the day in the nursery office (locked).

Handling Suspicious Messages (Phishing)

How to Spot Phishing Emails / Messages / Phone Calls
Phishing emails are designed to trick you into revealing personal information, passwords, or financial details. Watch out for these common signs:

Unexpected or Unusual Messages - You receive an email you weren’t expecting, especially about payments, accounts, or urgent issues. It may claim you need to act *immediately*.

Suspicious Sender Address - The sender’s email doesn’t match the organisation they claim to be from. It may look similar but with extra numbers, letters or strange domains.

Poor Spelling, Grammar, or Formatting - Many phishing emails contain mistakes, odd formatting, or unprofessional language.

Urgent or Threatening Language - Phrases like “Your account will be closed” or “Immediate action required” are common tactics.

Unexpected Links or Attachments - Links may lead to fake websites designed to steal login details. Attachments may contain malware, never open them unless you're sure they're safe.

Requests for Sensitive Information -Legitimate organisations will not ask for your passwords, bank details, or personal data via email.

Mismatched or Fake Branding Logos or layout may look slightly "off", low-quality, or inconsistent.

Any suspicious email should be forwarded to NCSC's suspicious email reporting service (e.g., report@phishing.gov.uk) if relevant.

If a staff member thinks they have responded to a phishing message (e.g., given password, clicked a link):

1. Change passwords immediately.
2. If financial data was involved, alert the relevant financial institution.
3. Report as an incident to the Cyber Security Lead.

Third Party Services

We have contracts with third party services and have access to their data protection, data breaches and security responsibilities.

When sharing newsletters or emails containing personal information, we use password protection or secure platforms such as Famly or our nursery email.

Training and Awareness

Office Employees and Managers will complete cyber security training.

Induction for new staff members will cover cyber-security.

Visual reminders and signposting for staff – using posters and infographics and regular communication to reinforce safe handling of devices and data.

Incident Response

- **Incident Definition**: Any suspected or confirmed breach of security, including data loss, unauthorised access, phishing, malware infection.
- **Reporting**: Staff must report incidents immediately to the Cyber Security Lead.
- **Containment & Recovery**:
  - Cyber Security Lead will coordinate containment (e.g., disconnect compromised device), assessment, and recovery (restore from backup if needed).
  - Document the incident: what happened, how it was discovered, actions taken, lessons learned.
- **Notification**:

- If personal data (children, staff) is compromised, we will follow our data protection policy.

Use of AI

'Artificial intelligence' (AI) is an umbrella term for a range of technologies based on algorithms (instructions that tell a computer what to do and how to do it) that are designed to complete tasks that previously required human thinking. If used safely, effectively and with the right infrastructure in place, AI can support everyday life of early years educators, however we must acknowledge the profound ethical concerns that must be mitigated in its use.

We do not use any personal data of children, families, staff members or intellectual property of the nursery, including its name, in the use of external AI tools. For example, no children's names, date of birth, images or anything else that is deemed personal data will be used on platforms such as Chat GPT.

We use the AI tools available on our online learning journal tool to support educators and leaders grammar. Staff should always review the text they want to use as an input before using the AI tool. We are mindful of the overuse of AI and the potential de-personalisation of communication so we will be monitoring posts and observations to ensure they are being reviewed appropriately before making a decision whether to continue using this feature or not.

We keep up to date with relevant documents such as Ofsted's approach to AI during inspection and regulation and regularly review and plan for the teams continual professional development regarding the use of AI.

https://www.gov.uk/government/publications/ofsteds-approach-to-ai/how-ofsted-looks-at-ai-during-inspection-and-regulation

Ethical Considerations

Whilst this is potentially a very helpful tool we must reflect upon the ethical concerns by the wider use of AI. 'The rapid rise in artificial intelligence (AI) has created many opportunities globally, from facilitating healthcare diagnoses to enabling human connections through social media and creating labour efficiencies through automated tasks.

However, these rapid changes also raise profound ethical concerns. These arise from the potential AI systems have to embed biases, contribute to climate degradation, threaten human rights and more. Such risks associated with AI have already begun to compound on top of existing inequalities, resulting in further harm to already marginalised groups.'

You can read more about this here: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics