Data Protection policy
Care chiefs children's nursery

Our childcare setting stores and processes information electronically relating to our business, our employees, children's doctors, parent's details and children's details, for the purpose of recording child attendance, performing accounting tasks, emergencies, health, safety and well-being of children, child learning, employee training, planning and client complaints and as a result is required to be registered under, and to comply with, the Data Protection Act 1998. Our childcare setting is registered with the Information Commissioner's Office who maintains a public register of data controllers and a general description of the personal information that we store and process.

As a part of the act our setting must adhere to certain guidelines:

1. The information that we keep must be relevant and the setting must know the purpose the information is used for, i.e. do we need to keep this information and why?
2. Individuals that the setting keeps information on must know that we have the information and must be able to understand what the information will be used for.
3. Individuals must be aware of the people or agencies that I am likely to share information with. (See Confidentiality below)
4. The information the setting holds must be secure whether it is held on paper or a computer.
5. Access to information must be limited to those who absolutely need to know it.
6. Information must be accurate and up-to-date.
7. Information that is no longer required must be deleted or destroyed.
8. Staff must receive training in their responsibilities under the Data Protection Act and must fulfil their responsibilities in practice.
9. The Information Commissioner's Office must be notified of any changes to the data held.

Our setting complies with these guidelines as follows:

1. The setting only requests and retains information from parents about themselves and their children that is absolutely necessary for the business tasks detailed above.
2. The setting uses a 'Childcare Application' to gather information about parents and children, the parent completes this and is aware that it will be stored and what it is used for.

June 2015 nursery manager

3. Parents are informed in our 'Confidentiality' clause the people or agencies that their information will be shared with or accessed by.
4. The information we keep is secured by a computer password and a database password. Data files are also password protected. Computers are locked in a secure building outside of business hours. Paper records are stored in a locked cupboard.
5. User level security is implemented at database level to ensure that users and Ofsted only have access to the information they need. Paper records are stored in a locked cupboard.
6. Information is initially gathered from parents and letters are sent out periodically to ask parents to check that their details remain accurate and up-to-date.
7. The setting must keep information on minded children for 8 years after termination; after this period electronic records are deleted and paper records shredded.
8. Employees are trained in their responsibilities under the Data Protection Act and are periodically monitored to ensure that they comply.
9. The Information Commissioners Office is notified about changes to the data we hold and our registration is checked and renewed every 12 months.

Right to Access Information

Our childcare setting stores and processes information electronically relating to our business, our employees, our clients and their children; individuals (subjects) whom information is held on have a right to see the data that is held, usually referred to as a 'subject access' request. An individual who makes a request in writing and pays a fee (Maximum £10.00) is entitled to be told:

- Whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed and whether it will be given to any other organisations or people.
- Given a copy of the information comprising the data.
- Given details of the source of the data (where available).

In most cases a subject access request must be responded to promptly and in any event within 40 calendar days of receiving the request. Under the right of subject access the individual is only entitled to request their own personal data and not data relating to other people unless they are acting on behalf of that person**.**

More information can be found at www.ico.gov.uk.

Privacy Notice – Data Protection Act 1998

AW Childcare Services Limited is the Data Controller for the purposes of the Data Protection Act. We collect information from you, and may receive information about you from your previous early years setting. We hold this personal data and use it to:

- support teaching and learning;
- monitor and report on child progress;
- provide appropriate pastoral care;
- assess how well the setting is doing, and
- under the duty of the Children's Act 2004 to co-operate with partners to improve the well-being of children.

This information includes your contact details, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information.

We will not give information about you to anyone outside the early years setting without your consent unless the law and our rules permit it.

We are required by law to pass some of your information to the Local Authority (LA) and the Department for Education (DfE) and health services.

Freedom of Information Act 2000

Right of Access

The act creates a general right of access, on request, to information held by public authorities. On receipt of a freedom of information claim a public authority has two corresponding duties. First, a duty to inform a member of the public whether or not it holds the information requested, and second if it does hold that information, to communicate it to the person making that request.

Any person can request information under the act; this includes legal entities such as companies. There is no special format for a request. Applicants do not need to mention the act when making a request. Applicants do not have to give a reason for their request; however, there are a number of exemptions.

Absolute exemptions

Exemptions designated "absolute exemptions" have no public interest test attached; relevant exemptions:

- Information that is accessible by other means
- Information contained in court records
- Information which (a) the applicant could obtain under the Data Protection Act 1998; or (b) where release would breach the data protection principles
- Information provided in confidence
- When disclosing the information is prohibited by an enactment; incompatible with an EU obligation; or would commit a contempt of court

Qualified exemptions

If information falls within a qualified exemption, it must be subject to a public interest test. Thus, a decision on the application of a qualified exemption operates in two stages. First, a public authority must determine whether or not information is covered by an exemption and then, even if it is covered, the authority must disclose the information unless the application of a public interest test indicated that the public interest favours non-disclosure.

Qualified exemptions can be sub-divided into two further categories: class-based exemptions covering information in particular classes, and harm-based exemptions covering situation where disclosure of information would be liable to cause harm.

Relevant Class-based exemptions

- Information held for purposes of investigations and proceedings conducted by public authorities
- Information covered by professional legal privilege

Relevant Harm-based exemptions

Under these exemptions the exemption would be likely to:

- Prejudice law enforcement (e.g., prevention of crime or administration of justice, etc.)
- Prejudice the auditing functions of any public authorities
- Endanger physical or mental health, or endanger the safety of the individual

- Prejudice commercial interests

Refusing requests

Vexatious requests

A public authority is not obliged to comply with a request for information if the request is vexatious. A request is considered vexatious if it is 'obsessive or manifestly unreasonable,' harasses the authority or causes distress to its staff, imposes a significant burden, or if the request lacks any serious value.