123 AFTER SCHOOL CLUB
PARENTS' ACCESS TO RECORDS

In order to work effectively 123 Club needs to gather information about staff, parents, children and professionals involved in the day to day running of the setting. By adhering to the policy, we will ensure that data is handled properly and confidentially at all times. Sleep.
The General Data Protection Regulation (GDPR) came into effect on 25th May 2018 replacing the current Data Protection Act 1998. It gives individuals greater control over their own personal data.

GDPR condenses the Data Protection Principles into six areas, which are referred to as the Privacy Principles. They are:
• You must have a lawful reason for collecting personal data and must do it in a fair and transparent way.
• You must only use the data for the reason it is initially obtained.
• You must not collect any more data than is necessary.
• It has to be accurate and there must be mechanisms in place to keep it up to date.
• You cannot keep it any longer than needed.
• You must protect the personal data.The GDPR provides the following rights for individuals:
• The right to be informed.
• The right of access.
• The right to rectification.
• The right to erase.
• The right to restrict processing.
• The right to data portability.
• The right to object.
• Rights in relation to automated decision-making and profiling.

As a childcare provider, we are the data controller. The data is our data that we have collected about the children and their families.

in Article 6 of the GDPR:
(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For the majority of data we collect, the lawful basis for doing so falls under the category of 'legal obligation' such as names, date of birth and addresses as we have a legal requirement to obtain this data as part of the Statutory Framework for the Early Years Foundation Stage. Some data we collect, for example, photographs, requires parents to give consent for us to do so. Where this is the case, parents will be required to sign a consent form to 'opt in' and are made aware that they have the right to withdraw their consent at any time.

Data retention
We will hold information about individuals only for as long as the law says and no longer than necessary. After this, we will dispose of it securely.

Security
We keep data about all individuals secure and aim to protect data against unauthorised change, damage, loss or theft. All data collected is only accessed by authorised individuals. All paper forms are kept locked away.

Privacy notices
All parents and staff are provided with privacy notices which inform them of our Policies around how and why we collect data, information sharing, security, data retention, access to their records and our commitment to compliance with the GDPR act.

Ensuring compliance
The members of staff responsible for ensuring that the setting is compliant Is MICHELLE SCOTT. Her main duties are to:
• Ensure that the provision is compliant with GDPR.
• Audit all personal data held.
• Ensure all staff are aware of their responsibilities under the law, this may include delivering staff training.
• Undertake investigations when there is a breach of personal data and report to the ICO.
• Keep up to date with the legislation.

Data breach
A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, accidentally lost or destroyed.
when a security incident takes place, we must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.
Personal data breaches can include:
· access by an unauthorised third party;
· deliberate or accidental action (or inaction) by a controller or processor;
· sending personal data to an incorrect recipient;
· computing devices containing personal data being lost or stolen;
· alteration of personal data without permission; and· loss of availability of personal data.

Where there has been a personal data breach, the person responsible for monitoring the setting's GDPR compliance will complete the Data Breach Reporting Form within 72 hours

Data Disclosure
The consent of the data subject will be obtained before the group discloses personal information to any organisation or individual.
All requests for disclosure will be in writing and telephone enquirers advised accordingly.
In cases of child protection, the law requires the disclosure of information, without consent, to relevant Health and Social Care Trust personnel and PSNI officers.If a request for information relating to child protection is received by telephone, steps should be taken to ensure that such information is disclosed to identifiable personnel (ie seek verification of identity) and only if the individual is entitled to receive that information (authorisation). It is advisable to disclose such information only to those known to be involved in child protection. If doubt exists, ask the enquirer to route enquiry through a known channel. Always call an enquirer back and be very alert if the number given is that of a mobile telephone. 123 Club reserves the right to refuse if we aren't satisfied that the call is authentic.
Requests from parents for a printed list of children's names/addresses will be politely refused.
Personal data (including images) will not be used in newsletters, websites or in other media without the consent of the data subject. The conditions outlined in will be adhered to strictly.
A record will be kept of any data disclosed so that the recipient can be informed should data be updated/altered at a later date.

Data Access
Data subjects have the right to access any personal data held about them. Any person(s) wishing to exercise this right must make a request in writing to the Data Controller.
The Data Controller will issue the appropriate form.
On receipt of the required fee and the completed and signed form, the designated Data Controller will make the information available. The information will be made available as soon as possible and within one-month period recommended by the Information Commissioner. This may be extended by a further two months where requests are complex or numerous.
If this is the case, we will advise you within the 30 day period explaining why the extension is necessary.
We reserve the right to refuse to respond to a request but will explain our reasons why and also inform you of the right to complain to the ICO without delay and at the latest within one calendar month.

The right to erasure
This does not provide an absolute right to be forgotten. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:-
• Data is no longer necessary.
• Individual withdraws consent.
• Individual objects and there are no legitimate interest for processing.

- The data was unlawfully processed.
- The data must be erased to comply with a legal obligation.
- The data relates to society services to a child. Request for information under Data Protection Act

Request for Access to Data - Child/Young Person
I, _____ wish to have access to Personal Data that _____ (name of group) has about my child or the child in my care.
Name of child: ……..
Date of birth: ……..
In the following categories (please tick as appropriate):
Health and medical matters
Religious information
Personal details including name, address, date of birth, etc
Other information (please specify)
Signed:
Date:
Name in capitals:
Address:
Postcode:Request for Access to Data - Any Adult
I, _____ wish to have access to Personal Data that _____ (name of group) has about me in the following categories (please tick as appropriate):
Health and medical matters
Religious information
Personal details including name, address, date of birth, etc
Other information (please specify)
Signed:
Date:
Name in capitals:
Address:
Postcode:Notice of Changes to Personal Information
Child/Young Person
Name of Parent or Guardian:
_____
Name of Child:
_____
With reference to the Data Protection Act (1998), please note the following changes to the above-named child/young person's personal information:
Signed:
Date:
Name in capitals:
Address:
Postcode:Notice of Changes to Personal Information
Adult
Name: ……..