Clutton Playgroup

Data Protection Policy

Aim: To store and use data about the children in accordance with the General Data Protection Regulations (GDPR), a new EU law that will come into place on 25th May 2018. It replaces the Data Protection Act 1998 and the changes will stay in place even after the UK leaves the EU in 2019.

GDPR will give individuals more control over their personal data.

Principles of GDPR

GDPR condenses data protection principles into 6 areas called the Privacy Principles.

1. We must have a lawful reason for collecting data and must do it in a fair and transparent way.
2. We must only use the data for the reason it is originally obtained.
3. We must not collect more data than is necessary.
4. The information must be accurate and there must be systems in place to keep it up to date.
5. We cannot keep it any longer than needed.
6. We must protect personal data.

We must comply with these principles and also show that the correct systems are in place to demonstrate how compliance with them is achieved. We will have to have written policies and procedures in place and follow them. There is an expectation that staff will be trained in data protection.

We do not need to have a Data Protection Officer as it is sufficient to have someone who will take the lead on our compliance programme. The Data Protection Co-ordinator will be ……..

Privacy notices:

When we collect data we must tell people how we are going to use it and who we are going to share it with. At Clutton Playgroup we hold information about the children in order to support their development, to monitor their progress, to provide appropriate care and to assess how well the setting as a whole is doing. This information includes contact details, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information. From time to time Early Years settings are required to pass on some of this data to Local Authorities (LAs), the Department for Education and Schools (DfES), and to other agencies that are prescribed by law such as the Qualifications and Curriculum Agency (QCA) and OFSTED.

Review date – October 2019

We must now inform people that they have the right to withdraw their consent for us to hold the information at any time and that they have a right to lodge a complaint with the Information Commissioners Office (ICO). These privacy notice must be communicated in plain and clear English.

Individual rights

Our setting must ensure that we have systems to allow individuals to exercise their rights which include:

- Telling people what data we collect and what we are going to do with it.
- Allowing them to see it after it has been collected.
- Making changes if it is incorrect.
- Removing it if we have no legal right to hold it.
- Not processing the information if they don't want us to.
- Informing other data processors if someone asks you not to use their data.
- Letting people take their data away.
- Taking account of objections to what we hold and do with their data.
- Allowing people to ask us not to make any automated decisions about their data.

In order to comply with these rights Clutton Management Committee will send a letter to each family setting out their rights and asking them to let us know if they have any concerns. We do not ask for any details that are not needed for the safety and well-being of the children in the group. We will also give information about who their data is shared with.

The Local Authority uses information about children for whom it provides services to carry out specific functions for which it is responsible. For example, the LA will make an assessment of any special educational needs the child may have. It also uses the information to derive statistics to inform various decisions. The statistics are used in such a way that individual children cannot be identified by them.

The Qualifications and Curriculum Agency uses information about children to administer national assessments such as the Foundation Stage Profile. Any results passed on to the DfES are used to compile statistics on trends and patterns of development. The QCA can use this information to evaluate the effectiveness of the national curriculum and the associated assessment arrangements, and to ensure that these are continually improved.

Her Majesty Chief Inspector for Schools and OFSTED use information about the progress and performance of children to help inspectors evaluate the work of Early Yeas Settings, to assist them in their self-evaluation and as part of the effectiveness of educational initiatives and policy. Inspection reports do not identify individual children.

The Secretary of State for Education and the Department for Education and Skills use information about children and Pupils for research and statistical purposes, to allocate funds, to inform, influence and improve education policy and to monitor the performance of the education and children's services as a whole. The DfES will feed back to Las information about children for a variety of purposes that will include data checking exercises and use in self-evaluation analyses.

Consent:

Clutton Playgroup will also have to be able to demonstrate that consent for collecting data was freely given, specific, informed and unambiguous. Silence, pre-ticked boxes or inactivity will not

suffice as permission. People will have to actively opt in. To clarify that permission was freely given Clutton Playgroup Committee will renew permissions with Parents and Carers.

Data Processing:

GDPR sets out the lawful basis for processing personal information. Using information to comply with a legal obligation or using it after the data subject has given their consent would meet the requirements. Other examples of where the processing would meet requirements would be if the information is needed to protect the interests of the data subject or where is might be necessary for the performance of a task carried out in the public interest.

Data Agreements:

GDPR places a requirement of the early years setting to ensure that any arrangements made with data processors are governed by written agreements. Early years Providers must only use processors which offer sufficient guarantees the processing with meet GDPR requirements. We are also expected to renegotiate any pre-existing agreements to ensure they meet the GDPR standards if they continue past 25th May 2018.

New Projects:

Data protection must be built into new projects and services. In certain circumstances risk assessments must be carried out to ensure that sufficient measures are in place to keep personal data secure.

Breach Notification:

GDPR introduces an obligation to report a data breach to the ICO within 72 hours of becoming aware of it. It would be good practice to notify the individuals concerned even though we do not store information that is high risk to the individual, e.g. if the compromised data could lead to identity fraud.

All personal information, including photographs, is kept at the Cabin, except when staff take the learning journals home to update them and to prepare their reports. Staff are fully aware of the need for confidentiality at these times.

Photos are printed at Jenny Bush's house and stored on her computer. The data is protected by Beachhead Management system which was recommended by CETSAT agile Technology.

Beachhead's Simply Secure Management System is a single, configurable, web-based management tool allowing you to remotely secure the vulnerable mobile devices in your organization, including those devices owned by employees. Built for iPhone and iPads, Android phones and tablets, Windows and Mac PCs, and USB storage, SimplySecure modules can be added instantaneously to your account/web console as you need them. Designed to be easy enough for an IT staff of one to deploy and manage, and transparent to users to promote maximum employee productivity, this innovative approach to device security dispels the reputation earned by other products in the market. And, because it's a service, the system can grow incrementally as you add more and different devices. Plus, there's never a need to buy any additional hardware or software to manage your security.

Features include:

Customizable reporting of status and device risks/conditions
Remote enforcement of password and security policy

Review date – October 2019

Full encryption of all sensitive data on the devices
Immediate data access elimination with instant, administrator-enabled remote restoration
Complete data wipe capability when devices are stolen
Broad range of both administrator-enabled and automatic security responses to threat conditions

The only people that have access to these details are members of staff, OFSTED during an inspection or Parents or Guardians. No other persons will have access to the children's files without first gaining the consent of parents or guardians.

This policy was written with guidance from an article written by Peter Donaldson, director of human resources at the Preschool Learning Alliance.

This policy was approved and adopted at a committee meeting held on _____

Signed _____ (Chair Person)

Review date – October 2019