Data Protection policy for staff

Sensitive personal data: This information includes personal information to the individual such as their ethnic origin, political options, health, sexuality, religious beliefs and cultural identity. Information which also included sensitive personal data is whether a child has SEN, is looked after under the Local Authority, there are current safeguarding concerns being investigated by the Local Authority, or whether the child has any additional support in school such as free school meals.

Personal data: Any information personal to the child such as name, address, contact details, attendance to the holiday club, and any financial information.

All information we hold at the club includes information about past and present children who attend/attended the club, parents/carers personal information, staff member's personal information, volunteer's personal information, and any other professionals who have visited the club.

Paper records:

- Do not leave any personal information around unattended. This, where possible should be kept in a lockable cupboard and only accessible to those who require it such as staff members.
- All paperwork should be kept secure at all times, and should not be accessible to parents, other children, or visitors.
- No sensitive data should be left visible on the desk for anyone to read.
- All information which is paper based such as children's register, medical information, trip information, allergies and any personal information such as contact number and addresses must always be returned to senior management at the end of the day.
- Any electronic documents which are printed should be collected from the printer immediately after. Children should not be asked to collect these from the printer.
- All personal data information should be disposed of securely. E.g. via a shredder or secure bin/bag.

Wifi and downloading:

- Do not save/download any personal data to your personal electronic items such as tablets, phones etc.
- All personal information downloaded should be on property owned by Little Munchkins such as a laptop or camera.
- Do not log into public wifi when handling any personal data.

Emails:

- Access to emails should only be by the senior management within the club.
- Do not open any emails from unrecognised email addresses, or if a warning sign for the attachment appears.
- Do not use any personal email accounts about correspondence for the club. The only email address which should be used is littlemunchkinsclub@outlook.com.
- Double check the address of the recipient, to ensure information is not being sent to the wrong individual as this could contact sensitive data.
- Use the 'bcc' feature when sending an email, if this is sent to more than one. This is to avoid displaying email addresses of other individuals in the group.
- When discussing a child within the email, initials to be used where appropriate when sensitive personal information is being shared such as medical condition or religion.

Devices:

- Ensure all devices are not taken off the premises without managements consent.
- If any devices are taken off the premises, such as camera on a trip, this is your responsibility to ensure it is safely returned to the club and locked away.
- Ensure all devices are locked when they are left unattended.

- If you are required to use any of the electronic devices, then ensure the device is password protected and no notifications are set to a preview being visible in a locked screen.
- All pictures taken of children should be done on a Little Munchkins Club device, after gaining consent from parents/carers.
- No images/videos should be taken on any personal devices.
- Do not download any applications on Little Munchkins Club devices without managements consent to do so.
- When working with any sensitive/personal data, be mindful of the position of the screen so it cannot be easily read by others.

Displaying data:

- Consent must be gained from parents before personal information is displayed such as pictures. Parents are able to consent to this via a photograph permission form.

Verbal disclosure:

- When required to have sensitive conversations, be mindful of the environment, as if done in an open space, there may be others around.
- As it is not always possible to take phone calls in private, be mindful of sensitive information being shared where someone may overhear.
- If there are visitors or parents present in the club, be mindful of personal information being shared about their child whilst others are around and may overhear.
- Do not discuss any personal information relating to other staff members, children, parents or visitors with friends or anyone outside of the Little Munchkins Club setting.

Additional data protection points:

- Only keep data for as long as it is required. Any data deleted needs to be consented by the manager.
- If you have to share any highly sensitive data, then try to do this over the phone or in person where ever possible.
- Remember data protection laws do not stop if you are reporting any safeguarding concerns. This information should be shared with the relevant individuals. You do not need anyone's consent to do this.
- If an individual requests to see the personal data we hold about them through a ';subject access request,' information your manager of this request.
- Inform your manager if you think personal information has been lost, stolen, accessed by an individual who should not have this, or you have wrongly shared any information.

Staff name: …….

Staff signature: ……..

Date: …….

This policy was adopted by: Little Munchkins Children's Club	**Date:**
To be reviewed:	**Signed:**