Just for Kidz
Nursery & Pre-School

E Safety Policy

Policy Statement

The internet is an accessible tool to children in early year's settings.

All early years settings have a duty to ensure that children are protected from potential harm both within and beyond the learning environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

Aims

- To offer valuable guidance and resources to early years settings and practitioners to ensure that they can provide a safe and secure online environment for all children in their care.
- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the early years setting.

Scope of Policy

This policy applies to all staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above mentioned groups, such as mobile phones or iPads/tablets which are brought into an early years setting. This policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site, such as a work laptop or mobile phone.

At Just for Kidz, we provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer. Children learn in an environment where security measures are balanced appropriately with the need to learn effectively. Our Nursery understands the importance of an E-Safety Policy.

Staff Responsibilities Practitioners (including volunteers)

Our E-Safety Lead is ______________________________

The role of the E-Safety Lead in our nursery includes:

- Ensuring that the E-Safety Policy and associated documents are up to date and reviewed regularly;
- Ensuring that the policy is implemented and that compliance is actively monitored;
- Ensuring that all staff are aware of reporting procedures and requirements should an E-Safety incident occur;
- Ensuring that the E-Safety incident log is appropriately maintained and reviewed regularly;
- Keeping up to date with E-Safety issues and guidance through liaising the local authority and attending regular training.
- Ensuring E-Safety updates, training and advice is available for staff, parents/carers and children.
- Liaison with Senior Designated Person(s) to ensure a coordinated approach across relevant safeguarding issues.

All staff have a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.

Broadband and Age Appropriate Filtering

Broadband provision is essential to the running of an early years setting, not only allowing for communication with parents and carers but also providing access to a wealth of resources and support. Many settings now use internet enabled devices, including iPad educational apps and games, to enhance the learning experience of children or as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available regardless of the size of the setting.

Filtering levels are managed and monitored on behalf of the setting by E-Safety Lead.

Email Use

Staff

- The setting provides all staff with access to a professional email account to use for all work related business, including communication with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- All emails should be professional in tone and checked carefully before sending, just as an official letter would be.

- Email is covered by the Data Protection Act (1988) and the Freedom of information Act (2000) so safe practise should be followed in respect of record keeping and security. All staff is aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy. All users must report immediately any email that makes them feel uncomfortable, is offensive, threating or bullying in nature.

Use of Social Networking Sites (advertising or parental contact)

Social networking sites (e.g. Facebook and Twitter) can be a useful advertising tool for early year's settings and can often be an effective way of engaging with young or hard to reach parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites. Best practice guidance states that:

- Identifiable images of children should not be used on social networking sites.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.
- Ensure that privacy settings are set to maximum and checked regularly.
- For safeguarding purposes, photographs or videos of looked after children must not be shared on social networking sites.

.

Please note: Just for Kidz Ltd does not currently use any social media sites for advertising or sharing images.

Mobile/Smart Phones

Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in nursery is allowed. Just for Kidz choses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used, in turn eliminating the following concerns:

- Staff being distracted from their work with children
- The inappropriate use of mobile phone cameras around children

Our aim is to have a clear policy on the acceptable use of mobile phones and cameras that is understood and adhered to by all parties concerned without exception. In order to achieve this aim, we operate the following acceptable use policy:

1. The nursery allows staff to bring in personal mobile phones and devices for their own use, however, these can only be used during break times and in the staff room only.
2. Staff bringing in devices to nursery must ensure there is no inappropriate or illegal content on the device.
3. All staff must ensure their mobile phones/devices are left inside their bag, throughout the contact time they have with children. Staff bags will be kept in the staff room.
4. Mobile phone calls may only be taken during staff breaks in the staff room.

5. If staff have a personal emergency, they are free to use the settings phone, or make a personal call from their mobile phone in the designated area.
6. If staff are in a situation where there is a family emergency where they may need to be contacted at any point during the day, staff should give relatives the nursery number and ask to contact them via the nursery phone.
7. Staff need to ensure management have up to date record on contact numbers and emergency contacts. This is the responsibility of individual staff.
8. All helpers/students/visitors will be requested to place their bag containing any mobile phones or devices in the office area, and to take any calls in this room away from the children.
9. during group outings, breakfast/after school walk, staff will use the designated Nursery Mobile phone only, not their personal devices.

It is the responsibility of all staff to be vigilant and report any concerns to the nursery manager/leader. Concerns will be taken seriously, logged and investigated using the LADO procedures (allegations against a member of staff)
The manager/owner reserves the right to check the image contents of a member of staffs mobile phone should there be a cause for concern over the appropriate use of any device. Should inappropriate material be found, our Local Authority Designated Officer (LADO) will be contacted immediately, alongside Ofsted. We will follow the guidance of the LADO as to the appropriate measures for the staff member's dismissal.

CAMERAS
Photographs taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form of recording their progression in the Early Years Foundation Stage. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.
To do this, we adhere to the following procedures:

1. Only the designated nursery camera is to be used to take any photos within the setting or on outings.
2. Images taken on this camera must be deemed suitable without putting the child/Ren in any compromising position that could cause embarrassment or distress.
3. All staff are responsible for the location of their designated camera and must keep it safe and secure at all times.
4. Images taken on the camera must be downloaded as soon as possible onto the nursery PC in the office.
5. Images must only be downloaded by the nominated senior member of staff (Mitra Ashab).
6. Photos will be printed and distributed to key persons to record in the Childs learning journey.
7. Under no circumstance at any time, must cameras be taken into the bathroom areas or nappy changing areas without prior consultation with the manager.

8. If photographs need to be taken in the bathroom, e.g. recording children washing their hands, the manager must be informed first, and staff to be supervised whilst pictures are taken.
9. When we have concerts or events where children will perform for their parents, parents will be asked not to record or take photos, as the nursery staff will take their own pictures which can be distributed to parents after the event.
Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

School Provided Mobile Devices

- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Photographs and Video

Digital photographs and videos are an important part of the learning experience in early years settings and, as such**,** staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos.

As photographs and video of pupils and staff are regarded as personal data in terms of the Data Protection Act (1998) we must have written permission for their use from the individual or their parent/carer.

Photographs taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form of recording their progression in the Early Years Foundation Stage. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.
To do this, we adhere to the following procedures:

1. Only the designated nursery camera is to be used to take any photos within the setting or on outings.

2. Images taken on this camera must be deemed suitable without putting the child/Ren in any compromising position that could cause embarrassment or distress.
3. All staff are responsible for the location of their designated camera and must keep it safe and secure at all times.
4. Images taken on the camera must be downloaded as soon as possible onto the nursery PC in the office.
5. Images must only be downloaded by the nominated senior member of staff (Mitra Ashab).
6. Photos will be printed and distributed to key persons to record in the Childs learning journey.
7. Under no circumstance at any time, must cameras be taken into the bathroom areas or nappy changing areas without prior consultation with the manager.
8. If photographs need to be taken in the bathroom, e.g. recording children washing their hands, the manager must be informed first, and staff to be supervised whilst pictures are taken.
9. When we have concerts or events where children will perform for their parents, parents will be asked not to record or take photos, as the nursery staff will take their own pictures which can be distributed to parents after the event.

Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

When taking photographs/video, staffs ensures that subjects are appropriately dressed and are not participating in activities that could be misinterpreted.

Storage of Images

- Images/films of children are stored only on Nursery devices.
- Staff are not permitted to use portable media storage of images (e.g. USB sticks) without express permission of the Manager.
- Rights of access to this material are restricted to the teaching staff within the confines of the Nursery.

Webcams and CCTV

Just for Kidz uses CCTV for security and safety. The only people with access to this area are the Managers and Directors.

Webcams are used by staff to attend online training and Zoom meetings.

Laptops/iPads/Tablets

Staff Use:

- Where staff have been issued with a device (e.g. setting laptop) for work purposes, personal use whilst off site is not permitted. The settings laptop/devices should be used by the authorised person only.
- Staff are aware that all activities carried out on setting devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.
- Staff will ensure that setting laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.
- Setting issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted and this must be acknowledged in the policy.

Children's Use:

- Laptop, iPad use must be supervised by an adult at all times and any games or apps used must be from a pre-approved selection checked and agreed by the Manager.
- Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device.

Applications (Apps) for recording pupil progress

In recent years, a number of applications (apps) for mobile devices have been launched which are targeted specifically at Early Years Practitioners and settings. Many of these apps allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

- **Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft**.

Just for Kidz Ltd makes use of the app: www.learningjournals.co.uk

Data Storage and Security

In line with the requirements of the Data Protection Act (1988), sensitive or personal data is recorded, processed, transferred and made available for access in nursery. This data must be accurate; secure; fairly and lawfully process; processed for limited purposes and in accordance with the data subjects rights; adequate, relevant and not excessive; kept no longer than necessary; and only transferred to others with adequate protection.

At Just for Kidz Ltd we specify how we keep data secure and inform staff as to what they can/cannot do with regard to data through this E-Safety policy. The E-Safety lead is responsible for managing information. ICT enables efficient and effective access to and storage of data for the management team, staff and administrative staff.

Just for Kidz Ltd complies with LEA requirements for the management of information in Nursery. Only trained and designated members of staff have authority and access rights to input or alter data.
The Nursery has defined roles and responsibilities to ensure data is well maintained, secure and that appropriate access is properly managed with appropriate training provided.

Approved anti-virus software is updated regularly.

All laptops and computers are password protected. All work email accounts are password protected. A secure email facility is available for staffs that need to send confidential information. Passwords should contain at least eight characters and contain upper and lower case letters as well as numbers. Passwords should be easy to remember, but hard to guess. Staff should not share their passwords with anyone; write their passwords down or save passwords in web browsers if offered to do so. Staff should not use their username as a password. Staff should not email their password or share it in an instant message. Staff should change their password if they think someone may have found out what it is.

Staff should be aware of who they are allowed to share information with. Clarification can be obtained from the E-Safety Lead. Sensitive information should only be sent via the secure email system. Don't assume that third-party organisations know how your information should be protected.

The use of unencrypted memory storage devices to store information of a personal sensitive or confidential nature is not permitted.

Staff should only download files or programs from trusted sources. If in doubt, advice should be sought from the E-Safety Lead.

Staff should lock sensitive information away when left unattended.
Unauthorised people should not be allowed into staff areas. Computer screens should be positioned so that they cannot be read by others who shouldn't have access to that information. Confidential documents should not be left out.
Staff should only take information offsite when authorised and only when necessary. On occasions when this is necessary, staff should ensure that the information is protected offsite in the ways referred to above. Staff should be aware of their location and take appropriate action to reduce the risk of theft. Staff should ensure that they sign out completely from any services they have used, for example email accounts. Staff should try to reduce the risk of people looking at what they are working with. Laptops should not be taken abroad (some countries restrict or prohibit encryption technologies).

Serious Incidents

If a serious incident occurs such as inappropriate content is accessed, the e safety incident log is made immediately and a nominated officer is informed. The use of classroom computers is suspended until fully investigated.

Useful links

- Data Protection and Freedom of Information advice: www. ico.org.uk

Incident Reporting

E Safety Incident Log

Details of ALL safety incidents to be recorded by staff and monitored monthly by the Provider/Manager.

Policy Composed by: Mitra Ashab
Date: 1.11.2021
Review: 1.11.2022