Information and Communication Technology and Online Safety

This policy aims to outline safe and effective practice in the use of technology and the internet. It provides safe and effective measures to enable children and adults to use Information and Communication Technology (ICT) resources in a safe way. This policy applies to all individuals who have access to technology and the online world. This includes children, parents/carers, Allsorts staff, Committee members, visitors, and students.

Learning about technology helps children to understand and feel empowered to use those technologies efficiently and safely. To ensure equality, all children and staff are encouraged to use and benefit from opportunities provided by a range of ICT. Some children may need extra support and guidance by giving reminders, prompts and further explanations to reinforce and develop each individual's knowledge and understanding of online safety. Up-to date training for all staff is therefore paramount.

Types of technology that can and will be used in the community that we must have an open awareness of are; texts, instant messaging, email, computers, laptops, the internet, chat rooms, blogs, social networks, podcasts, GPS, wireless/broadband, mobile phones (with Wi-Fi, Bluetooth, cameras, videos and many more), gaming (online games and games consoles), video broadcasts, music downloads, digital cameras, smart white boards, tablets and smart watches. Some of these have an individual sub policy (please see below).

Children and adults will be closely supervised online by having the technology in places of high visibility (unless data protection and confidentiality of others is at risk). Age appropriate websites will be closely monitored and viewed by an appropriate adult prior to being used by a child.

All adults should be aware that the risks involved when using ICT include:

- Prolonged exposure to online technologies, particularly from an early age.
- Exposure to inappropriate content, images and language.
- Making, taking and distribution of indecent images and 'sexting'.
- Cyber bullying.
- Grooming.
- Physical, sexual and emotional abuse.
- Addiction to gambling, gaming or pornography.
- Pressure from media and targeted advertising.
- Theft and fraud from activities such as phishing.
- Viruses, Trojans, diallers, key loggers, spyware and other malware (people can watch the children through webcams and cameras of tablets if hacked).
- Social pressure to maintain online networks via texting and social networking sites.
- Identity theft.

Allsorts and its staff members will take responsibility for providing online safety guidance and education to the children. Safeguarding support systems that will be put into place are; filtering controls, only using secure networks, passwords on devices, used of appropriate systems such as Famly and virus protection. New equipment will be checked before there is any use for either staff or children. This will promote safer use of online technologies both within the setting and the home environment.

Concerns, Reporting and Recording

For the above Safeguarding policy to be effective, online safety is a must and its procedures must be clear, agreed and respected. This is to keep everyone (especially the children) safe without limiting opportunities for exploration, creativity and innovation. Managing risks around technology will provide a better learning experience as prohibiting access to online gives a false sense of security as children will become vulnerable as they get older and will not feel empowered. Safeguarding is everybody's business and therefore the paramount concern is to ensure the safety and wellbeing of children – this includes their online safety. Any allegations of misuse or known incidents will be dealt with appropriately and promptly in line with the Allsorts misuse policy and disciplinary procedures. Other agencies shall be contacted where applicable

Staff

All staff are expected to use a range of technological resources to manage their roles as professionals; to be enabled to use the internet to research and communicate professionally; to use online systems (Famly) to track and record the progress of the children, to communicate with parents and carers through newsletters and to be able to manage administrative tasks and systems.

The online environment is a public space and therefore information shared online is available to all. Allsorts understands that anything published can be a permanent record. All data is recorded through Famly and the information is shared with the staff and the named parent/carer. We will then gain parents' permission to share information with others accordingly dependent upon the information (such as accidents, developments with other professionals, emergency services etc). Furthermore, we will gain parents' permission to use Famly as our online learning journey that holds children's personal data for their learning and development. Any personal use of technologies such as tablets and cameras will be open to scrutiny, monitoring and review. It is acknowledged that not every eventuality can be safeguarded against. All staff are responsible for reporting any concerns to the DSL

Staff should only communicate for professional reasons using the Allsorts methods of communication not their own social network or mobile devices, not give any personal details to children, be aware of policy if staff or volunteers feel that personal information has been compromised, be careful in communication that it is open to scrutiny to avoid any misinterpretation. Staff are also aware of the different emoticons and how these can be misinterpreted.

Passwords

Authorised users will have their own individual passwords. The equipment that can hold personal information will be locked when unattended to prevent unauthorised access, this includes Famly. Computers should be set to a time out if they become idol for a certain length of time.

Mobile phones

Mobile phones are not allowed on a staff member's person whilst working with the children. All mobile phones will be kept in a box away from the children and access only allowed at break times or end of shift away from children. If you chose to store your mobile phone at Allsorts we advise it being security marked, password protected and insured. No liability for loss or damage to anybody's mobile phone is Allsorts responsibility

No member of Allsorts should contact a child or a parent using their own personal mobile phone unless in an emergency.

All students, volunteers and visitors who are remaining in the setting for any length of time will also be asked to hand in their phone or keep it switched off or on silent in handbags etc out of the Preschool rooms. The manager or person in charge has the right to ask anyone to leave if they do not comply. Any parents who attempt to use their phone within a setting will be asked to leave immediately or switch off and put away their phone. Any mobile devices bought into the setting by another agency or visitor should not contain any inappropriate or illegal content

The risks in having mobile phones are; taking indecent images and distributing them, exploitation and bullying. Such misuse will have a negative impact on an individual's (both child and adults) safety, dignity, privacy and right to confidentiality.

Allsorts work mobile phone is used as a communication tool to enable text messages and calls to be made and received as and when needed. Its main use is for on short trips and outings. Only authorised staff may have use of the Allsorts work mobile phone and this will be monitored and open to scrutiny. Personal calls may not be made on this phone other than in circumstances that are agreed with the DSL and registered person.

Driving – If a staff member is driving during their working hours they must not make or take any calls whilst driving or text as this is illegal.

Tablets

Tablets are used within the rooms to take photographs of children, to carry out research, to write observations, or to share appropriate online content with children.

Tablets must be used in a safe and sensible manner.

Cameras/photos on tablets

Allsorts will gain permission in taking photos only from parent or carer not any other family member or friend – while child attends the setting. The parent or carer can withdraw their consent at any time.

Any photos taken of the children should be on cameras or tablets solely for the purpose of Allsorts use within the setting or on outings as part of the setting. These cameras and tablets should not leave the premises and should not be used for any other purpose unless the DSL and registered person are informed of short outings or trips.

Photo's stored on memory cards will generally be erased within 2 months of taking photograph then saved securely with access restricted. If personal cameras are needed to be used on whole Allsorts outings, permission must be gained from both the DSL and the Registered Person and the photos must be instantly downloaded onto Allsorts computers on return and the camera cleared.

Allsorts are aware that the press enjoy different rights under the Data Protection Act when using photos for journalism therefore; we will gain parent permission for photos and inform the press of what information they can publish.

At times Allsorts has other agencies to either take photos or videos of the Christmas play or school photos. Parent's permission will be asked for before this can be done for individual children. Furthermore, Allsorts will ask to see the relevant DBS checks.

If at open events parents want to take photos they will have signed on their contract (as they are not covered by Data Protection Act) that these photos/videos are for their own use and are not allowed to upload images of other children onto the internet. Allsorts has a right to withdraw consent at any time and images and filming must be open to scrutiny at any time

Allsorts staff are aware that the tablet cameras may be hacked and could have strangers videoing children in the setting. This will be closely monitored by all

Social networking sites

Staff, students, volunteers or other adults in the setting are not to discuss, mention, refer or allude to anything to do with Allsorts, its staff, children or its activities on any social networking sites. Comments made or alluded to will be strictly monitored and removed if deemed unsuitable. Any breach of this is likely to become a disciplinary issue.

Staff own social networks should not be shared with any child in their care.

Allsorts have Facebook pages for each of its settings. Parents must give permission for photos of their child to be used on these pages, and no names of children should be used.

Other personal Devices

Staff must declare if they have their own device on them at the setting. At present staff may wear a Smart watch if it does not connect to the internet.

No personal tablets are allowed into the setting unless in special circumstances where they have gained permission from the relevant people

Famly

Allsorts will maintain confidentiality and security of data regarding the safeguarding of children by ensuring parent permission for the use of Famly. Staff are only to access Famly during work and only to their own key children unless working as administration to the Famly system. The system will be strictly monitored and children will be archived on the system once the child has left and the relevant information has been passed to either the next setting and/or the parents

Parents will be informed how to access this information confidentially and only the management team and the individual child's key person can gain the information through Famly.

Website

Allsorts has its own website. This is updated and maintained internally, but hosted externally. Parents must give permission for photos of their child to appear on Allsorts' website.

Parental Involvement

Parents will be informed through the policies about online safety. The importance of online safety will be discussed with parents, especially when this may need highlighting to particular individuals or there is cause for concern.

Permission is asked for Allsorts to take any photos or videos of their children and communicated about where the images or recordings will be used ie Famly, advertising, social network etc.

ICT Misuse

Allsorts will ensure that any allegation, which is made in respect of intentional or unintentional misuse of any online technologies, is addressed in a responsible and calm manner. This includes any known or suspected breaches of the ICT Policy. Allegations will be dealt with promptly and sensitively. If it is thought that it is a Safeguarding incident, then the safeguarding policy and procedures come into effect.

In the event that a child accidently accesses inappropriate material, it must be reported to an adult and then both their DSL and registered person immediately. Appropriate action should be taken to hide or minimise the window. The computer should not be switched off, nor the page closed, in order to allow investigations to take place.

In the event of misuse by a child, Allsorts will inform the parent of the issue and if deliberate the child may be temporarily suspended from the activity. The parent/carer will be invited in to talk about the incident with a senior member of staff, the DSL or a committee member.

In the event that misuse is of a serious nature and the child is at risk of harm then safeguarding policies are put into place and applied

Forms of misuse are sharing inappropriate content with a child, taking photos in changing areas, taking phots of children partially dressed, cyber bulling, using videos for personal use, taking photos when a child feels uncomfortable, photos being taken in the wrong context.

For any information needed on misuse including incidents, serious incidents, illegal material and media attention please see

Visitors

All visitors will be informed of the ICT and online policy and must be adhered to.

For further information, you may access:

https://help-for-early-years-providers.education.gov.uk/safeguarding-and-welfare/internet-safety

https://www.internetmatters.org/schools-esafety/pre-school/

At present no CCTV is in use but will be reviewed if needed

Reviewed September 2022