Updated September 2025

Allsorts Childcare ICT Policy

Purpose

This policy aims to outline safe and effective practice in the use of technology and the internet. It provides guidelines 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 internet. This includes children, parents/carers, Allsorts staff, Committee members, visitors and students.

Types of technology we use within the setting

Within the settings, children have access to the following technology, on a strictly supervised basis:

- Tablets (for research use, taking photos or watching short video clips relevant to learning topics)

Staff have access to:

- Tablets (for recording information about the children, taking photos and research purposes).
- Company mobile phone (for use when out on trips).
- Company laptops and computers (for completing paperwork, printing and research purposes).

Technology used in the community

Staff and parents must be aware of the technology that children have access to or are exposed to in the wider community and must ensure children are supervised and risks minimised.

These types of technology include, but are not limited to:

- Home laptops and computers.
- Mobile phones, smart watches and tablets.
- Games consoles.
- Smart hubs, televisions and smart speakers.
- Virtual environments such as chat rooms, online gaming, webinars and zoom.
- Cameras, videoing equipment, podcasts and downloads.
- Connections such as Bluetooth, WIFI and the internet as a whole.

Risks associated with technology

There are many risks with using technology and these must be managed and minimised as much as possible.

Risks include, but are not limited to:

- Children using technology for prolonged periods of time.
- Children becoming addicted to using their devices.
- Children accessing inappropriate content.
- Grooming, bullying and abuse.
- Fraud, theft or phishing.
- Inappropriate influences or pressure to behave or look a particular way.
- Viruses, malware or hacking.

Measures in place to manage risks

Whilst in our care, we take the following precautions to manage the risks from using technology:

- Supervising children at all times when they have access to any technology.
- Ensuring any confidential data or information is stored safely and correctly.
- Ensuring all company devices are password/pin protected.
- Ensuring all company devices have the relevant virus protection.
- Ensuring all company devices have safety filters in place for search engines and web browsing.
- Staff will not use personal devices such as mobile phones or smart watches whilst in the room with children.
- Permission will be gained from parents before children's photographs are taken or shared.
- Ensuring relevant guidelines are adhered to in relation to storing of photos or information on devices.
- Allsorts have an appointed E-Safety Champion who ensures all relevant guidance is adhered to.

Staff personal devices

Staff should ensure that personal devices such as mobile phones and personal tablets are stored in the office of their setting and not taken into the room with the children.

Mobile phones should be turned on silent whilst stored in the office. Staff should provide the setting telephone number to anyone who may need to contact them in an emergency whilst at work, such as family or their child's school.

Students, volunteers or other visitors should also store their devices in the office.

Smart watches should not be worn whilst working in the room with the children. These must be stored in the office along with mobile phones.

Parent/carer technology useage whilst on site

Parents/carers are asked not to use devices such as mobile phones or smart watches whilst in the settings to safeguard the children in our care.

Social Media

Allsorts has a Facebook page for each of its settings which is managed and run by the Offices Manager.

Any photos uploaded onto the page are done so with parent's permission that was given when their child initially registered with Allsorts.

Staff should be mindful of their social media usage and ensure that any association with Allsorts that is referred to on their personal social media does not bring the company into disrepute or cause safeguarding or confidentiality issues.

Parents/carers are asked to voice any concerns they may have via Famly message, email or face-to-face, rather than use social media for this purpose.

Staff should not add parents as 'friends' on social media if they have only met through Allsorts. If staff know parents personally prior to them starting with Allsorts then management should be informed. Staff should declare any personal friendships with Allsorts parents each time they do their declaration form, or as soon as friendships are formed.

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.

Famly

Allsorts uses Famly for its management information system. The security of data on this system is ensured at all times.

Only registered users have access to their own child's personal information.

Staff are only to use Famly whilst at work and on company devices.