E Safety

Policy statement

At Tiggers Pre-school we believe that children flourish best when they are offered opportunity to experience using different forms of media and technology which is aimed at their own personal developmental ability. We ensure that access to this technology is safe and protected.

This policy is drawn up to protect all parties – the children, the staff and the pre-school and aims to provide clear advice and guidance on how to minimise risks and how to deal with infringements. The internet, digital communication and digital technology are an essential element in 21st century life for education, business and social interaction. As a pre-school we have a duty to provide developmentally appropriate experience ICT in its various forms to build a foundation on which children can develop their knowledge with internet, e-mail and computer use when they move into primary school.

The Internet is also used in the Pre-school to support the professional work of staff, to allow effective planning and to enhance the Pre-school's management information and business administration systems.

Procedures

We aim to teach children to use technology in a safe manner. We ensure the programmes that the children have access to are suitable for their development level and that we support their learning in this area.

It is the duty of the pre-school to ensure that every child in their care is safe, and the same principles should apply to the virtual or digital world. (please also see our Safeguarding Policy)

If the children have access to the internet it will be designed expressly for their use and will include filtering appropriate for their age.

The children will be limited on the amount of time they spend accessing the computer/tablets.

How will filtering be managed?

Internet access will be password protected and this password will only be known by the supervisor, systems support and co-chairs. The password will be change regularly. Staff will not know the password and therefore will not be able to access the internet on personal devices. The use of personal mobile phones in the setting by staff, parents and carers' is forbidden to ensure the safety of the children. (please see Mobile phone policy)

- Staff will always use a child friendly safe search engine when accessing the web with the children

- The children will be given clear objectives for internet use set as age appropriate.

- Children will be closely monitored when using the computer and the internet at all times, by supervising adults.

- Staff may view additional websites with the children, for example to look at sites related to topics they have been discussing. Staff must ensure they logout immediately after viewing the sites to restrict access for the remainder of the pre-school session.

- The pre-school will ensure that the use of internet derived tools and programmes by staff and the child complies with copyright law.

What will happen if unsuitable material appears on the screen?

The pre-school will take reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content together with the speed of change, it is not possible to guarantee that unsuitable material will never appear on a preschool device. The pre-school cannot accept liability for material accessed, or any consequences of Internet access.

However if unsuitable material does appear on a device:

- Staff will take reasonable measures to hide the screen by closing the lap top, quickly removing the tablet or distracting the children.

- Staff must report incident to the Supervisor and/or the Systems Support committee member immediately so that the filters can be reviewed. (Please also see our Safeguarding Policy)

Other ICT equipment

Tablets : These are available to children. They have no internet access and are pre loaded with age appropriate software

Preschool camera(s): this is used by the staff to evidence children's learning. It is the responsibility of the supervisor to ensure its safe use. Photographs from this camera are used in children's Learning Journals and occasionally on the website (With parental consent, Please see Parental consent form in Welcome pack). The memory card on the camera will be cleared on a regular basis.

Children's Video cameras and Staff video camera: footage the children take is shared with the children to increase their confidence with the use of ICT. This will not be uploaded on to the internet. The staff video camera is used as an observation tool and informs their Next Steps of Learning. It is also used in Peer observations. This will be monitored by the supervisor and the memory cleared regularly. This will not be uploaded onto the internet.

Games, hand held technology from home are forbidden to be brought into the pre-school by the children.

Emails

Children will not have access to e-mail

The preschool has a designated website and admissions email address for professional correspondence which is password protected. Parents are given this information when expressing an interest in the preschool.
The preschool recognises that the supervisor, staff and Management Committee will communicate via email outside working hours.

- The preschool advises that personal computers are locked with a security password.
- The names of children should be kept to a minimum.
- Correspondence will be written in a polite, respectful and non-abusive manner.
- Any abuse or breeches of confidentiality by any adults associated with the preschool is strictly forbidden, and will not be tolerated.
- All suspected cases must be reported, the preschool will record all incidents and act on them immediately.

Storage of Documentation on personal computers

Tiggers Preschool recognises that personal computers are used to create working documents for the preschool, in terms of Transition Reports and Next Steps for instance.

- All home computers must be password protected
- Work documents placed in locked folders
- Only acceptable use is permitted
- Personal details are kept to a minimum
- All confidentiality is assured, with breaches considered serious misconduct, and dealt with accordingly

Other relevant Policies:

Social Networking Policy

Safeguarding Children

Mobile phone, Camera and Video Recording Policy

Primary legislation

The Children Act 1989 - s 47
The Protection of Children Act 1999
Data Protection Act 1998
The Children Act 2004, 2006 (Every Child Matters)
Safeguarding Vulnerable Groups Act 2006
The Children (NI) Order
The Children (Scotland) Order

Secondary Legislation

Sexual Offences Act (2003)
Criminal Justice and Court Services Act (2000)
Human Rights Act (1999)
Race Relations (Amendment) Act (2000)
Race Relations (Amendment) Act (1976) Regulations
Rehabilitation of Offenders Act 1974

Protection of Freedoms Act 2012