Acceptable Use and E-Safety Policy

This policy and associated procedures were adopted by Chelford Village Preschool on October 10th 2022.

Date of last review: 15th September 2023

Date of next review: 15th September 2024

Version: 1.0

Version Control Table

Version	Date Reviewed	Reviewed By	Comments
1.0	10th October 2022	Katherine Bones	New Policy Adopted
1.0	15th September 2023	Katherine Bones	No Changes

Acceptable Use and E Safety Policy

Aim

Chelford Village Pre-School recognises that there are significant educational and social benefits associated with the use of the Internet, which has become an everyday tool to support the development and learning within education. However, the nature of such an ever-changing environment highlights the need for a regular review of how we use and manage such technologies. Alongside the educational benefits there will always be risks when using technology that is available to the public and such risks need to be highlighted to all our Pre-School's users.

This policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard all adults, children and young people within Our Pre-School. This policy should also provide support and guidance to parents/carers for the safe and responsible use of these technologies outside of our Pre-School. It explains procedures for any unacceptable use of these technologies by adults and children.

Roles and Responsibilities

Manager and Committee

It is the overall responsibility of the manager and the committee to ensure that there is an overview of E-Safety across the Pre-School, as part of our Safeguarding Policies and commitment to all users of the setting. The manager and committee, will ensure that any incident is dealt with appropriately and in accordance with our policies and procedures. Action such as informing the police, parents and or suspension will be taken if necessary. Please refer to our Safeguarding Policy and Disciplinary and Grievance Policy for further information.

Staff and adults in the setting

It is the responsibility of all adults within the setting to:

• Ensure that they know who the Safeguarding Leads are within setting, so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the LADO or Local Authority Designated Officer, in accordance with our Safeguarding Policy.

• Be familiar with the Behaviour, Safeguarding and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately.

• Alert the Managers of any new or arising issues and risks that may need to be included within policies and procedures.

• Use electronic communications in an appropriate way that does not breach General Data Protection Regulations (GDPR), May 2018.

• Remember confidentiality and not to disclose confidential information.

Online Safety

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world.

Terms such as 'e-safety', 'online', 'communication technologies' and 'digital technologies' refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks. The issues are:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm

I.C.T Equipment

- The setting manager ensures that all computers have up-to-date virus protection installed.
- Tablets remain on the premises and are stored securely at all times when not in use.

Internet access

- Children never have unsupervised access to the internet.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- Children are taught the following stay safe principles in an age appropriate way:
    - only go online with a grown up
    - be kind online **and** keep information about me safely
    - only press buttons on the internet to things I understand

- tell a grown up if something makes me unhappy on the internet

- Staff support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- All devices for use by children are sited in an area clearly visible to staff.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Personal mobile phones – staff and visitors (includes internet enabled devices)

- Personal mobile phones and internet enabled devices are not used by staff during working hours. This does not include breaks where personal mobiles may be used off the premises or in a safe place e,g, staff room. The setting manager completes a risk assessment for where they can be used safely.
- Personal mobile phones are switched off and stored in a locked office drawer.
- In an emergency, personal mobile phones may be used in the privacy of the staff room or at the front of the building with permission.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Members of staff do not use personal equipment to take photographs of children.
- Parents and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day. Visitors are advised of a private space where they can use their mobile.

Cameras and videos

- Members of staff do not bring their own cameras or video recorders to the setting.
- Photographs/recordings of children are only taken for valid reasons, e.g. to record learning and development, or for displays, and are only taken on equipment belonging to the setting.
- Camera and video use is monitored by the setting manager.

- Where parents request permission to photograph or record their own children at special events, general permission is first gained from all parents for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.
- Photographs/recordings of children are only made if relevant permissions are in place.
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk

Tapestry: Online Digital Learning Journeys

Chelford Village Preschool subscribes to Tapestry, a web-based software package through which key persons update their key children's learning journeys. The package itself is a specialised and secure piece of educational software that has been specifically designed for use by schools and early years' settings. Tapestry is overseen by the Managers who are responsible for updating children's, parents, and staff members' details. Individuals, including parents and staff have their own personal passwords and login details. Parents are asked to sign permission details on their registration form when their child starts. Parents must specify if they do/do not give their consent for their child's image to appear in other children's learning journals as either a photograph or part of a video. The registration form also specifies that parents must not upload any photos from their child's learning journeys onto Facebook or any other social networking sites.

Use of social media

Staff are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure the organisation is not negatively affected by their actions and do not name the setting
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting

- are aware that images, such as those on Snapchat may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who are able to access
- not accept service users/children/parents as friends, as it is a breach of professional conduct
- report any concerns or breaches to the designated person in their setting
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the educator and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed

Use/distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague is behaving inappropriately, staff advise the designated person who follow procedure 06.2 Allegations against staff, volunteers or agency staff.

Legal References

- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Obscene Publications Act 1959
- Criminal Justice and Public Order Act 1994
- Data Protection Act 1998 • Human Rights Act 1998
- Freedom of Information Act 2000
- Communications Act 2003
- The Children Act 1989
- What To Do If You’re Worried A Child Is Being Abused 2006
- Safeguarding Vulnerable Groups Act 2006
- EYFS Statutory Framework 2012
- Working Together 2013