INTERNET AND SOCIAL NETWORKING SAFETY POLICY

Safeguarding & Welfare Requirements: Child Protection
Providers must have and implement a policy and procedures to safeguard children.

POLICY STATEMENT

St. Eval Pre-School take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

PROCEDURES

Information Communication Technology (ICT) equipment:

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- The designated person ensures that safety settings are set on children's equipment to ensure that inappropriate material cannot be accessed

Internet access:

- Children never have unsupervised access if and when accessing the internet.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.

Children are taught the following 'stay safe' principles in an age appropriate way as part of their learning:

- *Only go on-line with a grown up*
- *be kind on-line*
- *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*

Designated persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.

- Children are not allowed to access social networking sites.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the designated lead.
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC

Email:

- Children are not permitted to use email in the setting. Parents and staff are not permitted to use setting equipment to access personal emails.
- Staff do not access personal emails whilst supervising children.
- Staff send personal information securely and share information securely at all times.

Mobile phones – Children:

- Children do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this will be removed and stored in the office until the parent collects them at the end of their session.

Mobile phones – Staff and Visitors:

- Personal mobile phones are not used by staff on the premises during working hours. Phones to be stored in bags and kept in office.
- In an emergency, where staff members may be expecting a personal call of significant importance, personal mobile phones may be used in an area where there are no children present, with permission from the manager. These will be placed in the kitchen in clear view of others.
- Staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- If members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children.
- Parents and visitors are requested not to use their mobile phones whilst on the premises. Visitors will be advised of a quiet space where they can use their mobile phone, where no children are present. For example, in the Office.
- Work-issued mobiles are to be used for work purposes only and access the 'Famly App' for children's observations. These devices will only ever be taken be taken off site for purposes of visits and data held on them transferred only to setting owned devices – such as office computers.

Cameras and Videos:

-Volunteers must not bring their personal cameras or video recording equipment into the setting. Staff may be asked to take photographs for advertising purposes, but the Sim cards will be supervised by a manager and removed and cleared when finished

- Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development, or for displays within the setting, with written permission received by parents. Such use is monitored by the manager.

- Special events, such as the Graduation Ceremony, Parents are advised at the event that photographs may be taken of other children and asked not to share these on social media.

- If photographs/videos of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name. Written permission must be sought for this.

Social Media:

- Staff are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.

- Staff should discourage parents to be added as friends due to it being a breach of expected professional conduct. However, we are aware that we live in a small community where this may happen. Under these circumstances no sensitive information will be shared.

- Staff may name the organisation or workplace within social media to promote our charity or fundraising events, if they do so, it must be in a way that is not detrimental to the organisation or its service users.

- Staff observe confidentiality and refrain from discussing any issues relating to work

- Staff should not share information they would not want children, parents or colleagues to view.

- Staff should report any concerns or breaches to the designated person in their setting

-If staff members are contacted by parents in relation to pre-school, the staff member will advise the parent that they are unable to discuss matters pertaining to pre-school, and suggest they contact the manager / deputy manager.

- Staff avoid personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to a child attending

- The setting may use social media to promote the business. This will always be done sensitively ensuring the safety of the children and adults and avoiding safeguarding risks. Express permission will always be asked for if identity is visable.

Electronic learning journals for recording children's progress (FAMLY APP):

- Staff and Managers must ensure all information kept on these files is secure at all times.

- Staff adhere to the guidance provided with the system at all times.

- Parents are not added to the secure system until they have signed an agreement of behaviour. Failure to follow the rules laid out will result in parents being banned from the system.

Use and/or distribution of inappropriate images:

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed
- Staff are aware that grooming children and young people on line is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

Further guidance - NSPCC and CEOP Keeping Children Safe Online training

Designated Safeguarding Lead (DSL) : Rachael Richards

Deputy Designated Safeguarding Lead (DDSL): Hannah Richards

All Policies to be reviewed annually.

Acceptance of Policy			
APPROVAL Signature: Name & Position: Rachael Richards - Manager Date:		AGREED Signature: Name & Position: On behalf of the committee Date:	
Review Record			
Reviewed by:	Position:		Date:
Reviewed by:	Position:		Date:
Reviewed by:	Position:		Date:
Reviewed by:	Position:		Date:
Reviewed by:	Position:		Date: