1.2.2 Online and ICT Safety (Staff, parents, volunteers, and children)

Policy Statement

With this policy we aim to outline the safe use of all forms of information and communication technology (ICT). This will enable all adults and children involved with the group to communicate and learn ICT safely. This policy helps to recognise the potential risks as well as the immense value of ICT. Mandy Goff/Amelia Joyner are the designated On-line Safety Leads. Amelia Joyner is also our Safeguarding Officer and Pre-School Leader, and she will ensure the policy is adhered to at all times. The leads will ensure the online safety of all staff, volunteers, and children although the day-to-day responsibility for inline safety may be delegated to other members of staff.

The Online Safety Leads: -

- Ensures that staff/volunteers have an up-to-date awareness of the setting's online safety policy and practices and incident reporting procedures.
- Takes day to day responsibility for online safety issues and have a leading role in establishing and reviewing the online safety policies/procedures.
- Offers advice and support for all users.
- Keeps up to date with developments in online safety.
- Communicates with parents/carers.

The Online Safety Lead is aware of online safety issues and the potential for serious safeguarding issues and is capable of managing them effectively.

This policy includes the acceptable use of the internet, e-mails, storage of documents, childrens' records and images and cameras.

Staff and Volunteers

- Digital communications with children and families are professional and only carried out using the official systems of the setting.
- They are aware of current online safety trends and issues.
- Staff sign an acceptable use procedure which is regularly reviewed and updated to include latest technology developments.

Children and Technology

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

Terms such as 'e-safety', '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 used
Conduct – personal online behaviour that increases the likelihood of, or causes, harm

Children need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Children should demonstrate positive online behaviours.

Internet Access

- Children never have unsupervised access to the internet.
- The setting manager ensures that risk assessments in relation to e-safety are completed.
- Reputable sites with a focus on early learning are used (e.g. CBeebies).
- Video sharing sites such as YouTube are accessed but checked by staff as appropriate.
- 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 safe
  - 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 computers 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 stored in the office. Smart watches are allowed to be worn, including fit bits, health trackers and apple watches but must be on airplane mode with notifications disabled during session times.
- In an emergency, personal mobile phones may be used in the privacy of the office 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.
- Staff do not take their mobile phones on outings.
- 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 – including smart watches**
- Staff are permitted to wear smart watches but they are not to be connected to the internet during work hours so staff are asked to put their device onto airplane mode and to disable notifications as these are a distraction during session times. All watches are checked for connection and to ensure they do not have a camera capability. NO WATCHES that are camera enabled are to be worn under any circumstances.

- 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

Practice

The use of technology is managed at the setting through: -

- Supervision of children when on-line
- When internet is used, we manage access to online content through appropriate filtering and adult supervision.

Education - Children

Children need help and support and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

- Key online safety messages will be reinforced as part of all relevant planned programmes of activities.
- Online safety issues will be discussed, when possible, in informal conversations with children.
- When the opportunity arises, children will be guided to understand that not everything on the internet is true or accurate.
- Staff/volunteers will act as good role models in their use of online technologies.

Some parents/carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's online experiences.

We will provide online safety information and awareness to parents and carers through:

- Letters, newsletters, website
- Providing links to relevant good practice information/websites for parents/carers.
- Involving families in celebrating online safety events e.g., Safer Internet Day.

ACCEPTABLE USE POLICY

The Internet

All computer users must understand that any connection to the internet offers an opportunity for non-authorised users to view or access corporate information. Therefore, it is important that all connections be secure, controlled and monitored.

Information passing through or stored on pre-school equipment, as well as details of the sites on the internet which have been accessed, can be monitored. Users should also understand the pre-school has the right to monitor and review internet use and email communications sent or received by users as necessary.

The pre-school has i-pads which are password protected. These are used in session with supervision. We may opt to use the Pre-School laptop as another way of learning about technology and for research in line with the curriculum and in line with the EYFS. In this instance the laptop camera will always be covered by the switch.

Staff will intervene immediately in the event of any inappropriate material appearing on screen.

Website

Images taken of children whilst at pre-school will not be posted online, with the exception of those posted on our parent gallery, which is done via the computer in the Administration Manager's office. Our blog and photos are security protected with a password which is made available to families and is amended regularly.

The four laptops in the office are connected to the internet and have an up-to-date virus checker installed which is purchased on an annual basis and is updated regularly.

Parents general permission is obtained prior to images being taken. Access to our website is public but alterations to the content are only possible using the administration office password.

Parents and Carers are asked not to post photos that feature other peoples' children on social media.

Facebook

The pre-school runs a Facebook account which parents can 'like' for updates etc. Photos on social media never contain any faces or identifying features of any children and are always anonymous. The Pre-School Leader and Administration Manager both regularly monitor the page.

There is a an additional parent private facebook group which is promoted via our website. Staff are reminded not to join this and the group is separate to the running of the pre-school and is co-ordinated by other parents. This group is monitored by the committee member with safeguarding responsibility.

Prohibited Use

Users shall NOT use the internet to view download, save, receive, or send material related to or including: -

- Offensive content of any kind, including pornographic material.
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, disability, or social and economic background.
- Threatening or violent behaviour.
- Illegal activities.
- Commercial messages.
- Gambling.
- Sports and/or entertainment sites, YouTube, Google (except as required under the curriculum e.g., Google, YouTube, CBeebies).
- Personal financial gain.
- Forwarding e-mail chain letters.
- Sending of unsolicited e-mail (known as spamming).
- Material protected under copyright laws.
- Sending corporate data to pre-school's customers or clients without authorisation.
- Use of the Internet in order to misrepresent yourself or the pre-school to others.
- Installing or running unauthorised executable files on the network.
- Sending broadcast network messages.
- Connecting any unauthorised computer or any item of network equipment or any other device to the computer.
- Disconnecting or connecting any networking cable, or any interference with any item of networking equipment.
- The use of computer hacking tools which may lead to instant dismissal and possible prosecution.

Responsibilities

Cullompton Pre-School staff and committee members are responsible for honouring acceptable use policies or Internet and e-mail services.

The Administration Manager, Pre-School Leader and SENCO are aware that sensitive information should be sent by secure email only.

Expected Behaviour

Staff who access social networking sites at home e.g., Facebook, You Tube, Twitter, should refrain from posting comments about Cullompton Pre-School, past/existing members of staff, children, or children's families. Unacceptable use will be challenged and in extreme cases this could result in dismissal. The sharing and promoting of pre-school posts and content i.e., fundraising events, job vacancies and similar is encouraged by all staff.

Staff are advised not to socialise on networking sites with families of children who attend Cullompton Pre-School or who have siblings who may attend in the future. Staff are warned of the potential complications and possible consequences. Cullompton Pre School would prefer that staff do not comment on posts by current parents. There may be occasions when a member of staff and a 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.

New parents will be advised that staff will be unable to accept new friend requests via social media networking sites for the duration of their family's connection with pre-school. New employees who are already 'friends' with a family, or families, that attend Cullompton Pre-School will be advised on appropriate conduct, and asked to share if they are contacted about a work issue online.

All staff, volunteers and students must use appropriate language and respect others when they post on social media sites.

Staff are given regular on-line safety updates and advice on their social media use.

Cameras

Staff may take photographs of children to complete their Special Book, or any other planning or staff related activity. Parents sign a consent form giving us permission to photograph their child for this purpose. All images are stored securely on the Administration Manager's computer, which is password protected. Some images of children will be posted on our website, parents sign a form to give us permission to do this. Under no circumstances would a child be named in any of the photographs.

Staff may only use a pre-school camera during session times to photograph children. The cameras are kept securely in the locked cupboard overnight and are kept safe but available during session time to capture spontaneous moments to support the observation requirements of the Early Years Foundation stage and to share with parents. Photos are deleted daily from all cameras. Photos and videos are deleted from iPad daily.

Occasionally, a member of the press may be invited to pre-school. Only children with consent from parents may be photographed and named.

All hard drives and computers will be password protected. Access to images and personal data stored on the pre-school's computer will be restricted by the Administration Manager to those entitled to use this information.

Occasionally photographs may be used for student and visiting practitioners' presentations, with parental permission. Professionals working with special needs children may also use photographs taken here to make resources to support transitions and individual activities.

Cullompton Pre-School is registered with the Information Commission's Office.

This policy was adopted at a meeting of	Cullompton Pre-School	name of setting
Held on	8th March 2012	(date)
Date to be reviewed	March 2013	(date)

Signed on behalf of the management committee	
Name of signatory	JO FELLOWS

Role of signatory (e.g., chair/owner)	Chairperson

This policy has an annual review period and, as such, will be reviewed and signed off at a management committee meeting of Cullompton Pre-School each year, as shown below.

Previously reviewed on:-	13th November 2017	by	Owen Jones Chairperson
Previously reviewed on:-	19th November 2018	by	Alex Fox Chairperson
Previously reviewed on:-	18th November 2019	by	Alex Fox Chairperson
Previously reviewed on:-	24th January 2022	by	Jack Madge Chairperson
Previously reviewed on:-	19th February 2023	By	Hannah Tilley

Reviewed by Staff on:	January 2024
Reviewed by Committee on:	19/04/2024
Date of next review:	April 2025
Signed on behalf of the Management Committee:	Naomi Cook
Name of Signatory (printed):	Naomi Cook
Role of Signatory (e.g., Chairperson)	Secretary