Safeguarding: E-Safety Policy

EYFS 2017 Safeguarding and Welfare Requirement: Child Protection
The safeguarding policy and procedures must cover the use of mobile phones and cameras in the setting.

This procedure also links to:

- Internet Policy (Employee Handbook)
- Safeguarding children procedure
- Whistleblowing procedure
- Acceptable use of technology policy
- Tablet Policy (where applicable)

Failure to follow this procedure may lead to disciplinary procedures being implemented.

Policy Statement
ICP Nurseries Limited is aware of the growth of internet use and the advantages this can bring. However, it is also aware of the dangers and strives to support children, staff and families in using the internet safely.
Our designated safeguarding leads responsible for coordinating action taken to protect children are:

[Insert name here]
[Insert name here]
[Insert name here]

ICP Nurseries Limited takes the safety of children and staff seriously and at each nursery there is a nominated E-Safety Lead.

The named E-Safety Lead for this setting is

_____

The E-Safety Lead's Role Includes:

- holding a designated safeguarding lead training certificate.
- completing E-Safety Training
- ensuring that only ICT equipment belonging to the setting is used by staff and children.
- ensuring all ICT equipment is safe and fit for purpose.
- ensuring all computers have virus protection installed.

- ensuring that safety settings are set to ensure that inappropriate material cannot be accessed.
- completing an ICP Nurseries Limited **E-Safety Audit (Appendix 16)** termly, ensuring all new staff have been inducted on the E-Safety Policy and, along with the Nursery Manager, ensure adherence to it.
- keeping a **Chronology Form (Appendix 7)** and reporting E-Safety incidents as per the **ICP Nurseries Limited Safeguarding Initial Report Form (Appendix 6)**.
- embedding an E-Safety agenda point in every staff meeting that also covers continual professional development, including covering children's learning and development.
- promoting an E-Safety culture and promoting the setting's E-Safety vision to staff, parents/carers and the local community.
- making sure staff receive relevant information about emerging issues, for example, keeping up to date with local and national E-Safety awareness campaigns and issues surrounding existing, new and emerging technologies.
- supporting E-Safety awareness amongst children and young people in the setting using the tools provided by ICP Nurseries Limited, e.g. Little Birds Internet Security Adventure. A copy of this should be on the computers or tablets used by the children.
- ensuring the **Technology Poster (Appendix 18)** is located on the entrance door. This must be adhered to at all parental or community events.

Internet Access

- Children do not normally have access to the internet and never have unsupervised access.
- If staff access the internet with children to promote their learning, written permission is gained from parents who are shown this policy.
- The E-Safety Lead has overall responsibility for ensuring that children and young people are safeguarded and risk assessments concerning E-Safety are completed.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet:
  - only go online with a grown up
  - be kind online
  - 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
- The E-Safety Lead will also seek to build children's resilience concerning 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.
- Second hand computers and ICT equipment are never used, as we cannot be assured that no inappropriate material is stored on it before children use it.
- All ICT equipment for use by children is located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.

- The E-Safety Lead will report any suspicious or offensive material, including material that may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported by the E-Safety Lead to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.
- The E-Safety Lead ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If the E-Safety Lead becomes aware that any child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.

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 or work email whilst supervising children.
- Staff send personal information by encrypted email and share information securely at all times.

Videoconferencing

ICP Nurseries uses Microsoft Teams for video calls and conferencing. Microsoft Teams enforces team-wide and organization-wide two-factor authentication, single sign-on through Active Directory, and encryption of data in transit and at rest.

Zoom may be used for training and development purposes, however due to restrictions in security Zoom must not be used for any communications where there is a need to share sensitive personal information about the children, families and colleagues that we work with.

Video conferencing (VC) services provide the ability to conduct real time video meetings that can cover one to one or one to many site locations. Some of the key benefits of a video conferencing service are:

- saving time - reduces unproductive time spent travelling to and from meetings
- the ability to quickly organise real time face to face meetings for critical decision making
- saving money - reduction for travel and expenses costs
- environmental benefits - a reduction of CO2 emissions

The following re are some key considerations that should be factored into the operational service to minimise any potential security breaches.

- Use strong passwords, and do not disclose them to anyone else.
- Do not reveal dial-in details to anybody but the authorised participants in the call.

- If your service includes a public profile, do not reveal any sensitive, private or confidential information in it.
- Locking calls once all participants have arrived to stop anyone else from joining
- Ensure effective and updated internet security software and firewall is running.
- Ensure you are using secure Wi-Fi. Do not rely on public Wi-Fi/hotspots being secure, but use 3G / 4G instead, or a VPN.

After the call, always replace the handset or, click 'End call' to ensure that what you say or do subsequently remains confidential.

Mobile Phones, Smartwatches and Recording Technology
The E-Safety Lead and Nursery Manager will ensure that any person entering the nursery understands ICP Nurseries Limited does not allow the use of mobile phones, smartwatches or recording technology in areas used by children. Under no circumstance MUST personal technology be used within the setting.

All verified visitors upon arrival will be shown the "Information for Visitors" card which outlines:

- The Emergency Evacuation Procedure
- Child Protection & Safeguarding of children, together with the name of the setting's Designated Safeguarding person
- Our policy for the use of mobile phones, cameras and recording devices in the setting

Persons working either permanently or volunteering in the setting must sign their mobile technology over and fill out the **Mobile Telephone, SmartWatch or Tablet Log Sheet (HS42)** that is in or near the Nursery Manager's office. All mobile technology will be stored in mobile phone lockers that are provided by ICP Nurseries Limited for ALL staff members, volunteers, contractors or suppliers whilst on duty. Mobile technology use is only permitted in the designated mobile phone area, which is clearly identified with the official **Mobile Phone Safe Zone Poster (Appendix 46)**. Under NO circumstances must any recording technology be used in any other area on the nursery premises – it must be switched off on entering the building. Failure to follow these rules may result in disciplinary action being evoked against the individual failing to follow them. Staff are welcome to collect their mobile technology during their breaks and use them in the designated area.

Visitors to the setting MUST not be left unsupervised under any circumstances and staff must be vigilant to the use of any mobile phone or recording devices that the visitor may have on their person. If, at any point, the visitor displays such a device staff MUST politely and professionally request the visitor removes the item immediately.

The E-Safety Lead and Nursery Manager reserve the right to check the image contents on a member of staff's mobile technology should there be any cause for concern over the appropriate use of it.

ICP Nurseries Limited also requests that visitors take no unauthorised photographs or videos of their, or other children at the nursery or on any nursery outings. In such an event, authorisation must be sought from the Nursery Manager.

Mobile Phones

Mobile Phones – Nursery Manager

Each Nursery is issued a Nursery Manager Mobile Phone. This may only be used by the Nursery Manager or Deputy Manager, for the purpose of high-quality photographs and videos for My Memory Book, displays, communication with other nurseries, sharing of good practice and marketing. Photos of children may be taken, but only where permission has been gained for the child's photo to be used for external publication. The battery must be charged nightly.

Mobile Phones - Central Office Staff

ICP Central Office Staff carry company issued mobile phones, for the purpose of communication in their role, gathering photographic information and sharing of good practice. Photographs and videos of children may be taken, but only where permission has been gained for the child's photo to be used for external publication.

If in the event the Nursery Manager or Central Office mobile phone is stolen or misplaced, either in or out of the nursery building, this must be treated as a Safeguarding Incident and must be reported to the ICP Company Safeguarding Lead and a **Chronology Form (Appendix 7)** of events MUST be created.

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 is removed and stored in a locked drawer until the parent collects them at the end of the session.

Mobile Phones - Outings

Each ICP Nursery is issued with 'outings mobile phones' usually enough for each room to be able to go on separate outings. These are only to be used during an outing with the children to call the nursery upon arrival at and departure from the destination and in the case of an emergency. The senior member of staff overseeing the outing is responsible for the outings phone. The battery must be charged nightly and remain on the nursery premises at the end of the day. Under no circumstance MUST personal technology be used on an outing.

Mobile Phones – Staff and Visitors

Personal mobile phones must not be used by staff and visitors in areas accessed by children and families during working hours. Mobile technology use is only permitted in

the designated mobile phone area, which is clearly identified with the official **Mobile Phone Safe Zone Poster (Appendix 46).**

Staff and visitor's mobile phones will be stored in the phone lockers provided during operational hours. In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager. Our 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.

Smartwatches

We believe our staff should be completely attentive during their hours of working to ensure all children in the nursery receive good quality care and education. To ensure the safety and well-being of children, we do not allow the use of wearable technology, including SmartWatches and fitness trackers which facilitate communication or have the capability to record sound or imagery, during working hours.

Staff must adhere to the following:

- Smartwatches can only be used on a designated break and then this must be away from the children, in the designated mobile phone area.
- Smartwatches should be stored safely in the mobile phone lockers at all times during the hours of your working day.
- During outings, staff will use mobile phones belonging to the nursery wherever possible.

Cameras and Tablets

ICP Nurseries Limited encourages the use of designated cameras and tablets owned by the nursery to photograph and video children in play scenarios, enabling staff to capture the learning and development of their key child or group. It is not permitted for persons to take photographs or videos of children on their personal device.

The E-Safety Lead and Nursery Manager should ensure the **Camera In Out Sheet (HS55)** and **Tablet Log sheet** is used at the nursery to track the use and whereabouts of the nursery cameras and tablets at all times.

The camera memory/SD card must be stored away in lockable storage when not in use. Photographs and videos of children that are transferred to the Nursery computer must only be stored on the Nursery One Drive, NOT on the desktop of the computer. The Checks and removal of images stored on the devices or card must be cleared and acknowledged on the **Camera In Out Sheet (HS55)** and **Tablet Log Sheet** at the end of each month – this is the responsibility of the E-Safety Lead and Nursery Manager.

Photos must only be printed at the nursery. Apps such as the 'Free Prints App' must not be used.

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 (see the Registration form). Such use is monitored by the manager.

If photographs or 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 or through being photographed in a sweatshirt with the name of their setting on it.

If in the event the nursery camera or tablet is stolen or misplaced, either in or out of the nursery building, this must be treated as a Safeguarding Incident and must be reported to the ICP Company Safeguarding Lead and a **Chronology Form (Appendix 7)** of events MUST be created.

Early Photography Programme
As part of our Early Photography Programme, designated cameras are provided for use by the children and can be taken on Nursery outings. These cameras are ordered through the Nursery's Childcare Manager.

When using a camera, children are often working independently, so we do not necessarily know what is in the images. On rare occasions, children may inadvertently take inappropriate images of themselves or others. Staff must review children's images on the camera and delete any unwanted ones before downloading them to a computer. (Once uploaded, they are often automatically backed up on another server, making it harder to erase them completely.)

In terms of permissions, the same criteria should apply to photographs taken by children as to those taken by practitioners. Parental permission is a must if the images are to be used in contexts such as on the Nursery website or in publications. Practitioners should explain fully the proposed use of the images and obtain written permissions from parents.

Electronic Learning Journals for Recording Children's Progress
Electronic Learning Journals are fully secure systems that can be accessed via an app or website, which not only allows parents to access information about their child's achievements within the nursery, but also enables parents to be active contributors to the journal, for example by sharing information about significant events within the child's home life. To ensure the journal is fully secure and only password holders can access the features, the following actions must be taken:

- Practitioners must seek permission from the nursery management team before using any online learning journal.
- A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
- Staff adhere to the guidance provided with the system at all times.
- Staff should log out of the Tapestry app or program when they are finished to maintain confidentiality.
- Staff should not share login or password details with any person not employed by ICP Nurseries.
- Staff should not share any information, photographs or videos relating to children with any person not employed by ICP Nurseries.
- Staff should take all responsible steps to ensure the safekeeping of any portable device and each tablet must be returned to the lockable storage unit and the end of every day.
- Tapestry must not be accessed using any private computer, off nursery premises, and all staff must maintain confidentiality and professionalism as per ICP Nurseries Confidentially policy.
- All entries on Tapestry remain the property of ICP Nursery.

Social Media

The term social media may include (but is not limited to) blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or services.

- The expectations' regarding the safe and responsible use of social media applies to all members of ICP Nurseries
- All members of the ICP Nurseries community are expected to engage in social media positively and responsibly.
- All members of the ICP Nurseries community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control children and staff access to social media whilst using setting provided devices and systems onsite.
- The use of social media during setting hours for personal use is not permitted for staff, unless on their break.
- The use of social media during setting hours for personal use is not permitted for children
- Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in the removal of internet access and/or disciplinary action.
- Concerns regarding the online conduct of any member of the ICP Nurseries community on social media, will be reported to the DSL and/or manager and will be managed in accordance with existing policies, including anti-bullying, allegations against staff, behaviour and child protection.

Official use of social media
ICP Nurseries official social media channels are LinkedIn and Facebook.

- The official use of social media sites by ICP Nurseries only takes place with clear educational or community engagement objectives and with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the manager and the marketing team.
- The nursery management team have access to account information and login details for our social media channels, in case of emergency, such as nursery closure.
- Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
- Staff use setting provided email addresses to register for and manage official social media channels.
- Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
- Public communications on behalf of the setting will, be read and agreed upon by a member of the marketing team.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and children will be informed of any official social media use, along with expectations for safe use and action is taken to safeguard the community.
- Only social media tools (LinkedIn and Facebook) that have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving children will be moderated if possible. If appropriate.
- Parents and carers will be informed of any official social media use with children; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- Any social media content will positively reflect the widest possible range of communities and promote a positive non-stereotyping environment that promotes dignity, respect and understanding of difference in all forms.

If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Sign our **acceptable use of technology policy.**
- Be aware they are an ambassador for the setting.

- Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure appropriate consent has been given before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any private/direct messaging with current or past children or parents/carers.
- Inform their line manager, the DSL (or deputy) and/or the manager of any concerns, such as criticism, inappropriate content or contact from children.

Staff personal use of social media
The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our **acceptable use of technology policy.**
- Any complaint about staff misuse or policy breaches will be referred to the manager, in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Reputation
All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or ICP Nurseries into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media services. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This may include, but is not limited to:

- Setting appropriate privacy levels on their personal accounts/sites to ensure that their information is only available to people they choose to share information with.
- Being aware of the implications of using location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Using strong passwords.

- Not accepting service users, children and parents as friends due to it being a breach of expected professional conduct.
- Avoiding 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 and a risk assessment and agreement in relation to boundaries are agreed.
- Ensuring staff do not represent their personal views as being that of the setting.
- Ensuring that staff are not wearing their uniform for photographs and videos posted on social media that are not related to official business.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online. Staff are expected to ensure that their social media use is compatible with their professional role and is in accordance with our policies, and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about children and their family members or colleagues, will not be shared or discussed on social media sites.

Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role. Staff must report any concerns or breaches to the designated person in their setting.

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 online is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

Please note, where indecent images of children or other unsuitable material are found, it is important that you do not investigate the matter or evaluate the material, as this may lead to evidence being contaminated, which can lead to criminal prosecution. The E-Safety Lead and the Nursery Manager must record any activity on the **ICP Nurseries Limited Safeguarding Initial Report Form (Appendix 6),** follow the **Safeguarding Children and Child Protection Policy** and immediately contact the ICP Nurseries Strategic Safeguarding Lead for advice.

Legislation

The Statutory Framework for the Early Years Foundation Stage, page 17, 3.6 states:

"Training made available by the provider must enable staff to identify signs of possible abuse and neglect at the earliest opportunity and to respond in a timely and appropriate way…. Providers must train all staff to understand their safeguarding policy and procedures, which should include inappropriate behaviour displayed by other members of staff including the inappropriate sharing of images".

The legal framework surrounding E-Safety is:

- The Computer Misuse Act 1990 (sections 1-3)
- Copyright, Design and Patents Act 1988
- General Data Protection Regulations 2018
- Malicious Communications Act 1988 (section 1)
- Obscene Publications Act 1959 and 1964
- Public Order Act 1986 (sections 17-29)
- Protection of Children Act 1978 (section 1)
- Protection from Harassment Act 1997
- The Equality Act 2010
- Regulation of Investigatory Powers Act 2000
- Sexual Offences Act 2003
- The Children Act 1989
- The Childcare Act 2006