ICT/E safety POLICY

Please also refer to Child Protection Policy, Code of Conduct, Data Protection Policy, Prevent Duty, Tapestry Policy, Photographic Policy Disciplinary Procedure and Data Management Plan.

Guidance

Keeping children safe in Education 2023

Working together to Safeguard Children (2015, updated July 2022)

UK council for Internet Safety – Safeguarding children and protecting professionals in early years settings: online safety considerations for managers and practitioners – 2019

National Cyber Security Centre. Early Years practitioners: using cyber security to protect your settings - 2021

ICT is embedded in children's everyday experiences such as supermarket bar codes, interactive television and computer games, microwave ovens, vacuum cleaners, dvd/cd players and traffic lights.

We are aware that some children notice, observe and want to know how such devices work. We are equally aware that some children will have little knowledge or experience.

ICT resources can be used to impact on children's learning in all areas of the curriculum through the use of resources such as floor robots and toys. These can be incorporated into opportunities for problem solving and co-operation. Similarly, the use of resources such as old telephones and computer keyboards can present creative learning experiences to enhance imaginative/role play.

We are committed to providing learning experiences in ITC by:

1. Understanding the different ways in which children learn and how ICT is only one of a range of learning tools to support and develop their learning.
2. Promoting inclusion through a rich and varied ICT environment.
3. Making sure all children can access a range of safe and appropriate ICT resources within the setting such as cd player, remote controlled/programmable floor robots/cars, old telephones, computer

with child-friendly keyboard and a selection of suitable and age appropriate games.

4. Encouraging a sense of self-belief and worth through a growing independence regarding the use of the resources at hand.

E- Safety

Box Pre School Playgroup has a commitment to keeping children safe and healthy and the e-safety policy operates at all times under the umbrella of the Safeguarding Policy. We are aware that there are four main areas of risk:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

- **commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The E-safety policy is the implementation of the Safeguarding policy in relation to electronic communications of all types and as part of that implementation the preschool does everything it can to limit children's exposure to the risks outlined above. The DSL (Designated Safeguarding Lead) takes the lead responsibility for online safety concerns and is responsible for:

- ensuring that staff/volunteers have an up to date awareness of the setting's online safety policy and practices and incident reporting procedures
- is responsible for online safety issues and reviewing the online safety

policies/procedures
- offers advice and support for all users
- keeps up to date with developments in online safety
- understands and knows where to obtain additional support and where to report issues
- ensures provision of training and advice for staff/volunteers
- receives reports of online safety incidents and keeps a log of incidents to inform future online safety developments,
- communicates with parents/carers
- monitors incident logs

Staff/volunteers
Responsible for ensuring that:
- they have an up to date awareness of the setting's online safety policy and practices
- understand and follow the procedures for reporting and recording online safety
- digital communications with children and families are professional and only carried out using playgroup procedures.
- young people in their care are aware of online safety

On Line Safety

Technology – Devices

Technology is an intrinsic part of day-to-day operations in our setting and is used in many valuable ways to contribute to the work of our setting. We use:

- **administrative computers**
- **mobile phone belonging to the setting**
- **laptops**
- **tablets**

We monitor the use of these devices and how they are used through supervision.

Security

Our setting has effective systems in place to ensure the security of devices, systems, images and personal devices. These are regularly reviewed and updated, in the light of constantly changing technology and new online security threats.

We have identified those devices that are vulnerable to theft or their contents being compromised and have ensured they are both secure and protected, both physically and technically. We do this through:
Having the latest operating system security updates installed

- Protection from theft, loss or physical attack
- Data being regularly and securely backed up
- Any removable media containing personal or sensitive data is secured through password and/or encryption
- All devices and networks used professionally can only be accessed through secure passwords assigned to individual appropriate users. This allows us to manage and identify who has access to our systems.
- All of our staff/volunteers are regularly trained and updated in the secure use of the devices we use in our setting.

Digital Images

Our setting uses digital images and video as a tool to record and inform families/parents/carers of the progress and activities of their children. The devices we use for recording images of children are provided by the setting for staff/volunteers to use professionally.

We gain written permission from parents/carers/families to record and use digital image and video of their children. Through this process, we respect their rights under the Data Protection Act 2018.

Staff/volunteers are aware of the safeguarding risk to children if the privacy and security of those images is compromised and we have measures in place to limit this risk and to respond to issues when they arise.

Our setting stores images securely and we meet legal requirements on how long we retain those images.

We share images with parents/carers and families through the secure on line platform - Tapestry

We publish clear guidance for parent'/carers' use and subsequent sharing of digital image/video that has been taken at the setting or at an event organised

by the setting (particularly if other children are included).
We have processes in place to respond to parental concerns about how images are used and shared.
We ensure:

- care is taken that children are appropriately dressed in images
- that they are not participating in activities that bring the setting or its individuals into disrepute
- that full names of children are not shared on any public-facing media

Children's safety online
Parents/Carers
Parents/carers play a crucial role in supporting their children in the use of good online safety practice. We take opportunities to help parents understand these issues by issuing information at induction as well as through newsletters, providing links to good practice websites, involving families in safer internet day.

- Parents/carers sign our data protection and use of data permissions.

Children
We have regular planned activities concerning safety on line such as digi duck. Staff model appropriate on line behaviours when using the internet. Children do not have unsupervised access to the internet at playgroup. When using the internet child friendly search engines such as Swiggle are used.

Responding to On Line Safety Concerns
We recognise on line safety issues when they arise and we have an established procedure to respond.
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from any setting. Other activities e.g. promotion of terrorism or extremism are also banned and could lead to criminal prosecution.
There are however a range of activities which may, generally, be legal but would be inappropriate in the context of the care of children, either because of the age of the users or the nature of those activities.
Our setting believes that the activities referred to in the following section would be inappropriate in a context of working with young children:

- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of

Children Act 1978

- Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003

- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008

- Pornography

- Promotion of any kind of discrimination

- threatening behaviour, including promotion of physical violence or mental harm

- Promotion of extremism or terrorism

- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the setting or brings the setting into disrepute

Activities that might be classed as cyber-crime under the Computer Misuse Act:

- Gaining unauthorised access to setting networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the setting

- Unfair usage (downloading/uploading large files that hinders others in their use of the internet)

- Using setting systems to run a private business
- Infringing copyright

Other activities

- On line gaming and gambling, on line shopping, using social media/messaging apps, video broadcasting

Our setting has clear and manageable procedures when dealing with misuse. They are dealt with quickly and proportionately and are recorded and well communicated. Where illegal misuse has been identified, it is immediately reported to the Designated Safeguarding Lead, and escalated through the setting's safeguarding procedures to the appropriate supporting agency (Police; Designated Officer for Allegations, MASH.) In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to the police whilst police and internal procedures are being undertaken.
Our response is defined and guided by the "online safety Incident Flowchart" – see appendix 1.

Incidents of misuse by staff/volunteers will be dealt with through our disciplinary procedure

Reviewing on line safety

We carry out an annual review of on-line safety improvement tools such as https://360earlyyears.org.uk/

Staff receive update training at least annually.

Mobile technologies

Mobile phones are not permitted within the Pre-school room. Staff are permitted to use their mobile phones in the cupboard area, but the taking of photographs on mobile phones is strictly prohibited anywhere in the Pre-school site. There is a playgroup mobile phone for use on trips. The camera on this phone has been disabled. Rules and guidance on the use of devices is communicated to visitors when they sign in.

The Pre-school laptop remains the property of the Pre-school and must be returned if a member of staff leaves the Pre-school or as required.

Any member of staff using their own laptop must adhere to the ICT/e-safety policy in all matters relating to the Pre-school.

Smart Watches

Smart watches must not be worn by staff on the premises.

On-line communications and social networking.

We use a range of online services to communicate with our community, that include:)

- Website
- Social media pages
- Closed messaging system - Tapestry
- Email

All communications take place through clear and established setting systems and will be professional in nature.

On-line chat rooms and social networking sites such as Facebook or Twitter will not be used at the Pre-school. Staff will not discuss individual children or their setting on facebook, twitter or any other social networking site.

Facebook and Instagram

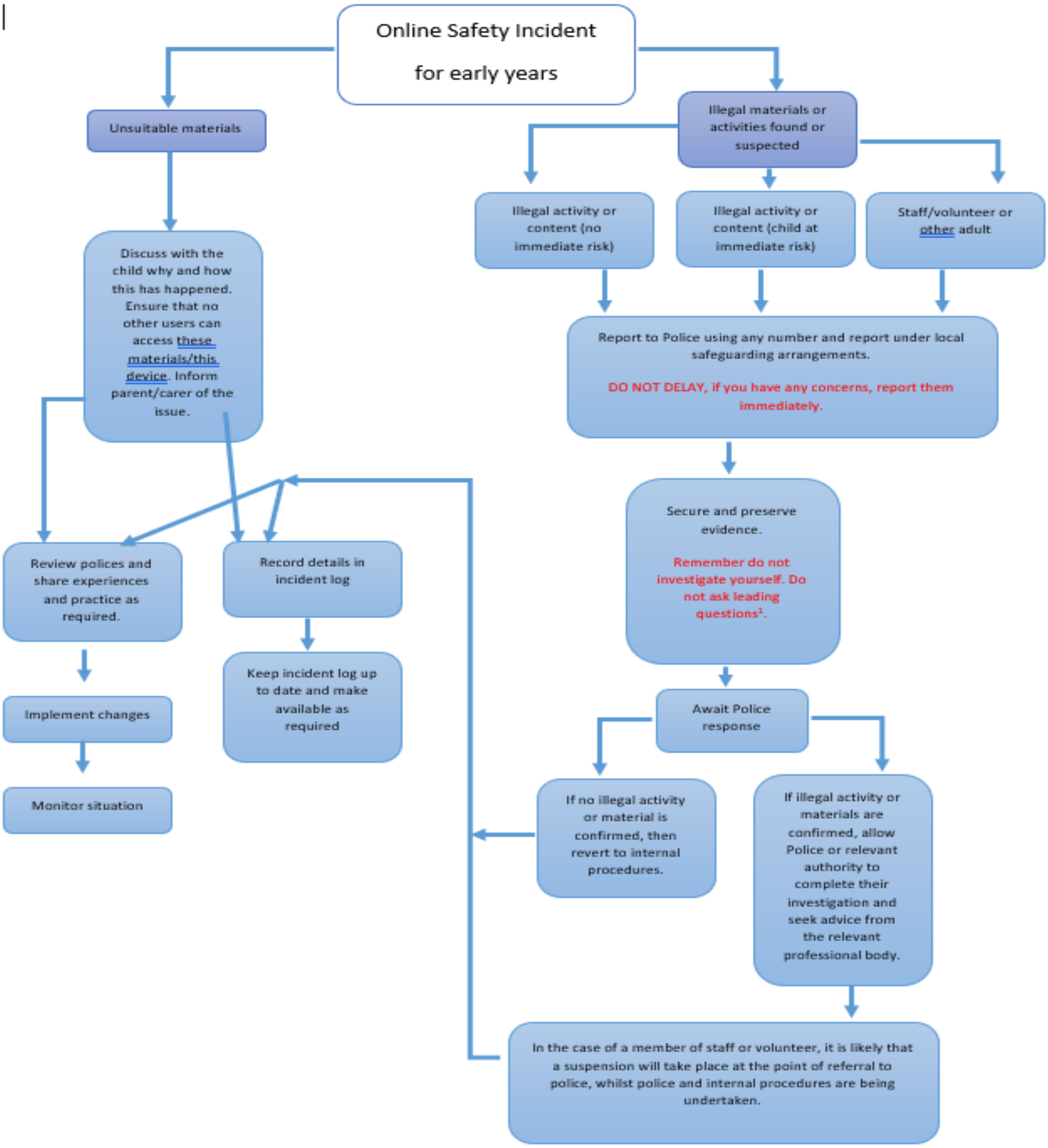
There is a public face book and Instagram account used for publicity purposes which is administered by the setting manager. The tone and content of this is professional and appropriate to the audience. These are accessed via the office computer. Parents give their permission for photographs of the children to be used on these sites. Digital communications by staff will be professional and respectful at all times. Users must declare who they are in social media posts or accounts. Anonymous posts are not allowed. Unacceptable conduct will be reported to the DSL and escalated where appropriate. The setting manager or Chair of the Committee will respond to journalists making contact regarding posts.

Video conference meetings

Some meetings are held via video conferencing calls. Only participants who are invited are allowed to join the call which is password protected. The participants are asked not to record any of the meetings. Children will not be included in video conference calls.

This policy will be reviewed annually or more regularly in the light of any significant new development. Should serious online incidents take place, the following external persons/agencies should be informed.
Designated Officer for Allegations (DOFA)
Local Authority Safeguarding (MASH)
Police
Information Commissioners Office

Appendix 1 Flowchart for responding to online safety incidents


Online Safety Incident for early years
Unsuitable materials
Illegal materials or activities found or suspected
Illegal activity or content (no immediate risk)
Illegal activity or content (child at immediate risk)
Staff/volunteer or other adult
Discuss with the child why and how this has happened. Ensure that no other users can access these materials/this device. Inform parent/carer of the issue.
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Review polices and share experiences and practice as required.
Record details in incident log
Implement changes
Keep incident log up to date and make available as required
Monitor situation
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.