Online Safety Audit for Early Years Providers

When conducting an Online Safety audit, there are several key areas to consider. The following audit has been organised into key areas to help each Early Years Provider to conduct a comprehensive assessment of Online Safety practices with their own setting. Please note this audit outlines many aspects of practise to be considered, but it is not an exhaustive list and there may be other factors within your own setting to consider.

Policies and Procedures	Yes	No	Actions to take
Online safety policies and procedures within the setting are up-to-date, comprehensive, and aligned with statutory guidance and best practices.			
Policies and procedures in place within the setting cover all aspects on online safety such as acceptable use policies, data protection, privacy, and consent.			
The setting's safeguarding policies and procedures include all electronic devices such as smart watches or any other device as developed with imaging and sharing capabilities, not just mobile phones, and cameras.			
Safeguarding policy and procedures, relating to the use of both personal and your setting's mobile phones and cameras are upheld within the setting.			
Effective systems are in place which ensure that children using technology and accessing the internet in the setting are always supervised by staff.			
Devices used by staff and children belong to the setting and personal devices are not used.			
Policies procedures and practices with the setting are regularly reviewed and updated in line with emerging risks and technological advancements.			

Risk assessment	Yes	No	Actions to take
Potential risks related to online activities within the setting are identified, these include risks associated with internet use, social media, online communication, and digital devices.			
Risks associated with internet use, social media, online communication, and digital devices are evaluated and appropriate measures are taken to reduce the impact of these risks.			
Filtering and monitoring systems	**Yes**	**No**	**Actions to take**
Technical safeguards such as content filtering, firewalls, and secure networks are in place throughout the setting.			
Websites, apps, and search results are always checked to ensure they are appropriate in terms age ratings and content.			
All devices (computers, tablets, etc.) have appropriate security and privacy settings and these are set to the highest level.			
Monitoring and Reporting:	**Yes**	**No**	**Actions to take**
There are established procedures for monitoring online activities within the setting and there is a named person who oversees internet usage and reports any incidents.			
Regular checks of all equipment are conducted by Leaders, Managers, and all staff to ensure appropriate access and use.			
The use of each IT item within the setting is logged, and accurate records are kept of when practitioners and children use them.			
Age-appropriate time limits are set for children who use devices in the setting, and these are monitored and reviewed regularly.			

Working with children	Yes	No	Actions to take
Online safety is integrated into the settings curriculum. For example, children engage in age-appropriate discussions and activities that teach them about safe internet use.			
Children are taught about their rights and responsibilities online.			
Staff understand how the use of devices to access the online world supports children's learning and development and can explain this to children, parents, and other professionals.			
Staff model safe internet use and language and encourage children to follow their example when using it themselves.			
Staff regularly talk to the children about keeping safe online and what to do if they are worried.			
Resources such as stories, videos and images are used throughout the setting to support children's understanding of how to stay safe online.			
Children are encouraged to be critical thinkers, respectful digital citizens, and active participants in their own safety.			

Working with Parents	Yes	No	Actions to take
The setting communicates with parents and shares information about online safety with them regularly.			
The setting involves parents in online safety discussions and provides resources and workshops to help them understand how to protect their children online.			
The setting considers what online risks children may be exposed to at home, e.g., vulnerability to radicalisation or other safeguarding risks and works with staff, children, and families to raise awareness of these.			
Staff Training and Awareness:	**Yes**	**No**	**Actions to take**
Staff are knowledgeable about online risks and how to mitigate them.			
Staff are provided with regular training sessions to keep them informed about the latest threats and safety measures and regulatory or sector updates.			
Staff know how to ask for advice when needed and are aware of where to find further advice and support about online safety.			
All staff receive regular supervision which provides opportunities for them to: • Share any concerns (including safeguarding concerns) which relate to children and staff. • Identify solutions. • Receive coaching and mentoring			

Remember that online safety is an ongoing process, and regular reviews and updates are essential.

Adapt your practices based on emerging risks and technological advancements.