Warwickshire Early Years Quality, Inclusion, SEND and Safeguarding

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.

It is also important to remember that technology changes all the time, whether functionality, risks, or appropriate settings, so regular review of policy, procedure and practice is essential.

Policies and Procedures	**Yes**	**No**	**Actions to take**
The setting has an up-to-date online safety policy (whether standalone or section within your settings safeguarding and child protection policy)			
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 wearable technology (e.g. smart watches, smart glasses) or any other device as developed with imaging and sharing capabilities, not just mobile phones, and cameras. The policies and procedures apply to all staff, parents, and visitors.			
Safeguarding policy and procedures, relating to the use of both personal and your setting's mobile phones and cameras are upheld within the setting.			
Clear policies which outline expectations for staff taking imagery of children are in place and fully implemented throughout the setting. these policies cover the device to be used, checking parental consent, ensuring images do not humiliate or show children in any state of undress etc.			
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.			
Staff are aware that any discussion of online safety, planned or ad hoc, by staff or visitors, may lead to a disclosure and must be dealt with in line with safeguarding procedures.			
All staff understand how to report online safety concerns			
All online safety concerns are followed up in an appropriate and timely manner in line with setting safeguarding policy and procedures.			
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.			
safety controls are appropriately in place on every device in the setting- these are checked regularly to ensure they are not disabled.			
All apps/games/websites/online tools used within the setting are checked for appropriateness by the setting's management team prior to use.			
Websites, apps, games, online tools, and search results are reviewed regularly 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.			
Device settings are checked regularly to ensure imagery and content on these is appropriate. These checks recorded and appropriate actions taken in response to these.			
Age-appropriate time limits are set for children who use devices in the setting, and these are monitored and reviewed regularly.			
Cyber security	**Yes**	**No**	**Actions to take**
The setting and all staff are aware of and adhere to clear procedures for secure data handling, password protection, and device use. Early Years practitioners: using cyber security to protect your settings			
A named staff member has responsibility for overseeing cyber security practices.			
Staff receive regular training on cyber security, including recognising phishing attempts, safe email use, and secure handling of digital information.			
Staff know how to report a cyber security concern or incident			
The setting has a clear process for reporting cyber breaches, data leaks, or suspicious activity.			
Records of cyber incidents are kept and reviewed to inform improvements.			
Parents are informed appropriately if data involving their child has been compromised.			
The setting has a documented Cyber Security Recovery Plan outlining how to respond to and recover from a cyber incident			

Children's personal data is stored securely and accessed only by authorised staff.			
Cloud-based platforms or online learning journals are GDPR-compliant and covered by a data processing agreement.			
Regular backups of critical data are completed and stored securely.			
Strong password protocols are in place (minimum length, complexity, regular changes).			
Passwords are **not shared** between staff and are stored securely.			
Devices automatically lock after a period of inactivity.			
Managers in the setting receive training and regular reminders on cyber security best-practice (passwords, phishing, reporting and more)? This training is shared with the team and put into practice in office practice and across the setting.			
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.			
Teaching and learning surrounding digital literacy is current and relevant to the setting and children's needs and experiences.			
Children are taught about their rights and responsibilities online, in an age-appropriate way.			
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 age-appropriate stories, videos and images are used throughout the			

setting to support children's understanding of how to stay safe online.			
Children in the setting are supported in an age-appropriate way to tell staff if they have an online safety concern.			
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. For example, the setting may remind parents about how to set controls on their home internet/ phones /devices. Appropriate time for technology, healthy habits about device use, guidelines for bedtimes, devices remaining downstairs, etc.			
The setting is proactive in engaging with parents and involves them in online safety discussions, 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 are comfortable with making the most of ad hoc opportunities to discuss and learn when online safety conversations arise with children or parents?			
Parents are signposted to age and stage appropriate programmes/games which support their child's current interests and stage of development.			
Staff Training and Awareness:	**Yes**	**No**	**Actions to take**
All staff receive online safety training as part of the safeguarding training schedule. This includes online safety scenarios to support staff learning			
Staff are knowledgeable about online risks and how to mitigate them.			
DSL's have received training in how to ensure internet safety (outlined in Annex C of EYFS 2025) and this training has been cascaded to the staff team.			

Staff are provided with regular training sessions to keep them informed about the latest threats and safety measures, regulatory or sector updates. Training provided also focuses upon specific incidents relating to general behaviour, risks or harms which have or may have occurred within the setting.			
Staff receive regular training on cyber security, including recognising phishing attempts, safe email use, and secure handling of digital information.			
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.