UK Council for Internet Safety

Safeguarding Children and Protecting Professionals in Early Years Settings

Online Safety Considerations for Managers

February 2019

UK Council for Internet Safety

This document is to help managers of early years settings (including wrap around care for the early years age group) ensure their online safeguarding practice is in line with statutory requirements and best practice. It may be helpful for managers to access and share with staff the *'Online Safety Guidance for Practitioners'* guidance.

Safeguarding Children and Protecting Professionals in Early Years Settings: Online Safety Considerations for Managers is a working document and we would appreciate your feedback. You can report on the guidance and your use of it by completing this survey which will close on 4th April 2019.

- All early years providers in England must follow the Early Years Foundation Stage (EYFS); there are different early years standards in Scotland and Wales.
- Providers must have regard to the government's statutory guidance 'Working Together to Safeguard Children' 2018 and to the 'Prevent duty guidance for England and Wales' 2015.
- Maintained nursery schools must have regards to 'Keeping Children Safe in Education' (KCSIE) 2018 statutory guidance; other childcare providers may also find it helpful to refer to this guidance.

Policies and Procedures

Why do early years settings need to consider this?

- EYFS 2017
  - If providers have concerns about children's safety or welfare, they must notify agencies with statutory responsibilities without delay
  - The setting's safeguarding policy and procedures must cover the use of mobile phones and cameras in the setting.
  - There is an expectation that children can access technology and use it safely.
- Ofsted 'Inspecting Safeguarding' 2018
  - Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being.
  - Leaders of early years settings implement the required policies with regard to the safe use of mobile phones and cameras in settings.

Managers should evidence that:	**Managers should ensure that all staff:**

• Online safety is recognised as part of the setting's safeguarding responsibilities
  ○ *The Designated Safeguarding Lead (DSL) should take lead responsibility for online safety concerns.*
• Online safety concerns are reported to the DSL, recorded and actioned.
• Children are enabled (at a level appropriate to their age and ability) to share online concerns
• The child protection policy includes procedures to follow regarding online safety concerns
• Their settings policies cover:
  ○ Safe and appropriate use of personal devices, wearable technology, mobile phones and cameras.
  ○ Acceptable and appropriate use of technology within the setting
  ○ Expectations regarding professional boundaries/behaviour of staff, including communication via social media
• Policies and procedures are easily accessible to staff and parents/carers
  ○ *For example, published on the setting's website*.
• Staff and parents/carers are consulted and actively involved, as far as possible in the development of policies
• Policies have been reviewed and approved by the management team/committee or equivalent
	• Understand their safeguarding responsibility and are clear about how it fits into their role on a day to day basis
	• Have read and understood the setting's policies relevant to online safety.
	  ○ T*his should include an Acceptable Use Policy (AUP) as part of the settings code of conduct.*
	• Are familiar with the setting's policies and procedures regarding safe technology use with children.
	• Are aware of the policy regarding staff contact outside of work;
	  ○ Communication with learners, parents/carers and colleagues should be professional and take place via official setting communication channels e.g. work provided emails/numbers to protect both staff and learners
	  ○ Communication should be transparent and open to scrutiny.
	• *Settings may find it helpful to access 'Guidance for safer working practice for those working with children and young people in education settings'* Understand that it is recommended that staff do not accept friend requests or communications from learners or their family members (past or present).
	  ○ *If there is a pre-existing relationship, this should be discussed with the DSL and/or the manager, who will need to consider how this is managed, provide staff with clear guidance and boundaries and record action taken.*
	• Understand and follow the procedures for reporting and recording online safety concerns, in line with the child protection policy.
	• Make use of home visits to inform their understanding of a child's context with regards to technology within the home. (e.g. how much and in what ways is tech used within the child's family life?)
	• Are aware that if they or another member of staff are targeted online, for example online bullying or harassment they should inform their line manager.
	  ○ *Managers may find it helpful to access the DfE 'Cyberbullying: Advice for headteachers and school staff' guidance.*

	• Are clear on the internal and external reporting mechanism regarding online safety concerns.
	  ○ Staff should always involve the DSL who will be able to make decisions about how and when to escalate a concern.
	  ○ *DSLs and staff should know how to contact:*
	  ■ *your local Multi-Agency Safeguarding Hub if they have a safeguarding concern about a child.*
	  ■ *the Internet Watch Foundation (IWF) if settings need to report illegal images. (child sexual abuse material)*
	  ■ *the Child Exploitation and Online Protection centre (CEOP) if they are worried about online abuse or the way that someone has been communicating online.*
	  ■ *the UK Safer Internet Centre Helpline for Professionals or the NSPCC for further information.*
	• Know how to access the settings whistleblowing policy and the NSPCC whistleblowing helpline.

Infrastructure and Technology

Why do early years settings need to consider this?

- Prevent Duty (2015)
  - Schools (and registered childcare providers) in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering".
- Ofsted ‘Inspecting Safeguarding’ 2018
  - Appropriate filters and monitoring systems are in place to protect learners from potentially harmful online material

Managers should evidence that:

- They are aware of how and why technology is used within the setting by staff and children
  - *This should include types and number of devices, if they are connected to the internet and if so, how (e.g. Wi-Fi)*
- Access to the setting’s network and IT infrastructure is secure
  - Such as use of passwords, screen locks, protected devices if removed from site
- Appropriate filtering and monitoring are in place and the setting has documented how decisions have been made
  - *Advice regarding appropriate filtering and monitoring is available from the UK Safer Internet Centre*
- Access to setting’s devices is managed and monitored
- Setting’s devices are kept securely and in line with data protection requirements.
- Physical safety of users has been considered e.g. posture of children/staff when using devices.
- Personal data is managed securely online, in accordance with the statutory requirements of the General Data Protection Regulations (GDPR) and Data Protection legislation.
  - *This should include considerations given to the use of online learning journals or apps if used.*

Managers should ensure that all staff:

- Appropriately supervise children whenever they are using devices
- Check apps, websites and tools prior to using them with children, this should include checking the results of searches
- Use age appropriate apps, websites and online tools with children
  - *There are details of useful websites that will provide links to appropriate content at the end of the document*
- Model safe practice when using technology with children
- Ensure data is shared online in accordance with the settings data protection responsibilities

Education and Training

<table>
<tr><td colspan="4">Why do early years settings need to consider this?
EYFS 2017
Providers must train all staff to understand their safeguarding policy and procedures and ensure that all staff have up to date knowledge of safeguarding issues.
Ofsted ‘Inspecting Safeguarding’ 2018
Staff, leaders and managers oversee the safe use of electronic and social media by staff and learners and take action immediately if they are concerned about bullying or risky behaviour.</td></tr>
<tr><td>Managers should evidence that:
The DSL has accessed training/information to ensure they understand the unique risks associated with online safety for early years children and have the relevant knowledge and up to date capability required to keep children safe online</td><td>Managers should ensure that all staff:
Are provided with quality and up-to-date online safety training on a regular (at least annual) basis, including at induction.
Are aware of the UKCIS framework (Education for a Connected World) which provides information about the skills and competences that children and young people need to have with regards to online safety from the age of 4 upwards.
Know how to report a problem and when to escalate a concern.
Are aware that civil, legal or disciplinary action can</td><td>Managers should ensure that all children:
Receive age appropriate, progressive and embedded online safety education throughout the curriculum.
Use age appropriate tools and resources.</td><td>Managers should ensure that parents:
Are given opportunities to develop their knowledge of online safety issues for early years children.
Are offered support to help them talk about online safety with their children in an age appropriate way.
Are signposted to appropriate sources of support regarding online safety at home.
Are supported by the setting if they experience an online safety concern.</td></tr>
</table>

	be taken against staff if they are found to have brought the profession or institution into disrepute. • Are aware that under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material. • Are aware of the need to manage their digital reputation, including the appropriateness of information and content that they post online, both professionally and personally. • Discuss online expectations and behaviour with their friends and colleagues ○ *For example, have they discussed what photos of them can and cannot be shared by their friends on social media.*		

	• Are aware that no matter what privacy settings are used, anything posted online can become public and permanent and could be misinterpreted and/or used without their knowledge or consent.		

Standards and Monitoring

Why do early years settings need to consider this? • Ofsted 'Inspecting Safeguarding' 2018 ○ Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being.
Managers should evidence that: • Policies are updated at least annually, and following any local/national changes • The setting regularly monitors and evaluates online safety approaches *e.g. reflecting on concerns and updating practice* • Staff are trained and provided with regular (at least annual) updates on online safety issues

Additional Information and Support

Many local authorities and grids provide in depth guidance and template policies to support managers and designated safeguarding leads within early years settings; check to see what support and training is available locally to you.

The following national organisations provide information:

- Childnet: For a range of educational materials and resources for use with children, parents and teachers
  - www.childnet.com/resources/social-networking-a-guide-for-teachers-and-professionals
  - www.childnet.com/parents-and-carers/hot-topics/keeping-young-children-safe-online/?tempid=1326955#
- DfE Data Protection Toolkit for Schools: For information on what schools need to do in order to comply with data protection regulations
  - www.gov.uk/government/publications/data-protection-toolkit-for-schools
- Information Commissioners Office (ICO): For information around data protection and GDPR

    - www.ico.org.uk/for-organisations/education/
- Internet Matters: For a range of materials for parents and teachers
    - www.internetmatters.org/schools-esafety/pre-school/
    - https://www.internetmatters.org/advice/0-5/
- NCA-CEOP: Education resources for use with children, parents and professionals and advice on safeguarding children from sexual abuse
    - www.thinkuknow.co.uk
    - www.thinkuknow.co.uk/parents
    - www.ceop.police.uk/Safety-Centre
- NSPCC:
    - www.nspcc.org.uk/onlinesafety
- Parent Zone: For a range of education materials and resources for use with children, parents and teachers
    - www.parentzone.org.uk/
    - Parent Info - https://parentinfo.org/
- UK Safer Internet Centre: For a range of education materials and resources for use with children, parents and teachers, UK SIC helpline for professionals who are working with children and young people
    - www.saferinternet.org.uk
    - www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/professional-reputation

Acceptable Use and Policy templates:

- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety
- https://swgfl.org.uk/products-services/online-safety/resources/online-safety-policy-templates/
- safepolicies.lgfl.net

This document has been bought to you by the UKCIS Education Working Group made up of the following organisations: