Guidance

Safeguarding children and protecting professionals in early years settings: online safety guidance for practitioners

Published 4 February 2019

1. Why does online safety matter to early years settings?

Ofcom's 'Children and Parents Media Use and Attitudes Report' (2018 – released in January 2019) found that:

- 1% of 3-4-year olds have their own smartphone and 19% have their own tablet
- 52% of 3-4-year olds go online for an average of nearly 9 hours a week
- 45% of 3-4-year olds use YouTube

It's important that early years settings ensure children are learning about the world around them and how to keep themselves safe online.

2. Why does online safety matter to me as an early years practitioner?

You play an essential role in helping young children learn the foundations of safe online behaviour. Even if children don't have access to technology within your setting, they may be using it at home, with their friends or in other public spaces.

Children are naturally curious in understanding the world we live in; it is our responsibility to enable them to do so, including helping them to recognise the value of technology and use it safely. Role modelling safe use of the internet should become part of our everyday practice.

Online safety is also highlighted within the Early Years Foundation Stage (EYFS) and Early Years Inspection Handbook.

Early Years settings are increasingly using devices, such as tablets, directly with children. This can be a great way of role modelling positive use of technology; however, if the activity isn't suitably planned it can cause issues.

3. What online risks might children in early years settings experience?

Early years children could be at risk of…

Content
(what they may see):

- Exposure to inappropriate videos, pictures or messages which might upset, worry or frighten them
- Imitating harmful or inappropriate behaviour they see online
- Searching for inappropriate content on purpose or stumbling upon it by accident. This would include using voice activated tools to search for content
- Inadvertently giving apps or websites permission to share their location or other personal information
- Spending real money via in-app or in-game purchases

Contact
(who might communicate with them):

- Being abused online (including sexually) by people they don't know, such as when gaming or using video chat
- Being abused online (including sexually) by people they know, such as friends and family members
- Sending images or information to people on the device's contact list

Conduct
(how they might behave):

- Exhibiting unhealthy behaviours and boundaries around their use of screens
- Being unkind to each other online as well as offline; this could be using mean words or by excluding others from their games
- Using words or terminology which are not appropriate for their age
- Engaging in unhealthy relationships
- As part of natural development, early years children may exhibit curiosity about their own and others' private body parts; if this occurs via technology children may be at risk of taking inappropriate or indecent images and videos of themselves – the Brook traffic light tool can help practitioners to determine whether sexual behaviour is normal healthy sexual development or harmful behaviour which is a cause for concern.

4. Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- Children in Early Years should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.
- Make use of home visits to inform your understanding of how technology is used within the home and the context of the child with regards to technology.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately.

For more information and practical advice, access the Childnet 'Educators pack for online safety awareness'

5. What online risks might children experience at home?

Risks could be posed to early years children because of the online behaviour of their parents/carers; this could include oversharing information about their children (or other children) online, and could, for example, include information which could identify a child or the nursery that they attend. Whilst sharing of images of children is a matter for parents and carers, care should be taken with privacy settings so there is some control over the image and who has access to it.

Some parents/carers could also place their children at risk due to their own personal vulnerabilities, for example they may be at risk of exposure to radicalisation. Additionally, children could be neglected because of their parents or carers overuse of the internet, or because of parents or carers failing to safeguard them online. See the NSPCC definitions and signs of child abuse document for further information.

You may also be a source of help and support for parents or carers about keeping their children safe online at home; some useful links which might be helpful can be found below.

6. What online safety resources are there for early years children and parents or carers?

6.1 Resources for settings to use for education

Childnet: Free Online Storybooks for early years and KS1 pupils

- Smartie the Penguin
- Digiduck Stories

Thinkuknow:

- Resources for early years and KS1 pupils from NCA-CEOP

UKCIS

- Education for a Connected World' Framework - this framework provides information on the skills and competences that children should have across 8 different areas of online safety

7. What do I need to be aware of when using social media in my personal life?

Using social media can be great but it can have risks for early years practitioners. The boundaries between the offline and online world are easily blurred; this can have potentially serious consequences for professionals.

7.1 Know your setting's policy and procedures

- Make sure you read and understand your setting's policies and procedures fully; use of social media may be covered in your code of conduct or "Acceptable Use Policy".
- If your setting uses social media as a communication tool with parents/carers, ensure you follow the guidance set out in your policies, such as not sharing photos without consent or using your own personal devices to share content on behalf of the setting.
- If your setting uses online learning journals, make sure you understand how these should be used safely and in line with your setting's data protection obligations.
- Make sure you understand your setting's policy regarding using work provided devices; be clear about how your setting allows work devices to be used or not used.
- If you are unsure of the policies and procedures in your setting, you should contact the Designated Safeguarding Lead (DSL) to find out where you can find this information.

7.2 Protect your online reputation

- Content posted online can be copied, shared or misinterpreted and can potentially be public and permanent. This can influence personal and professional perceptions about you, both positively and negatively.
- It is important to role model positive behaviour and be professional online; posting derogatory comments is never acceptable. Staff should uphold the reputation of their setting, professionally and personally. Disciplinary or legal action could be taken if you post something online which brings the profession or your setting into disrepute.
- Ask yourself when posting pictures or comments online; "would I say or do this in a face to face situation?" and "would it be appropriate for a child, their parents/carers or my manager to see this?". If the answer to either of these questions is no, it's probably best not to share it online in the first place!
- Check in with your friends and family about your online reputation; it's important that they understand what photos of you can and can't be posted on social media.

7.3 Manage online relationships

- You should not add parents of children at your setting as friends online; this can blur professional relationships and put you at risk of allegations. If there is a pre-existing relationship or situation which means this is not achievable, you should discuss this with the DSL at your setting and/or your manager so that they are aware and can give you advice.
- Do not give out your personal contact details to children or parents/carers; professional communication should always be through a work provided email, setting-approved digital platform or phone number.
- If you are concerned about something you see on social media, such as comments posted by a parent, make sure you report it to your DSL. If you are concerned about content posted by a colleague, follow your setting's allegations policy.

8. What should I do if I'm worried about a child or a colleague online?

If you are concerned about a child online, follow your child protection procedures and report and record to your DSL or your manager.

You can also contact a helpline for support and advice:

- Professionals Online Safety Helpline – Advice and support for professionals working with children with any online safety issues children in their care may face – 0344 381 4772 or helpline@saferinternet.org.uk
- NSPCC helpline – Advice and support for anyone who is worried about a child or needs information about child protection – 0808 800 5000

Be aware that early years children may take or share photos of their private body parts; these photos would likely, in a legal context, be considered to be indecent images of children. If you are aware of indecent images of a child, do not print, forward, save or share these images (this is illegal); report concerns immediately to your DSL.

9. What should I do if I have a concern?

Here are some important things to consider in the event of a concern about a child:

- If you are worried about a child for any reason, it is important to tell someone straight away. Follow your setting's child protection policy and report concerns immediately to the DSL so that the correct steps are taken from the start.
- Ensure that you are familiar with reporting procedures in your setting and that confidentiality is not promised to the child, or parent or carer in question as this could compromise subsequent investigations.
- Ensure that the child's own words are used and are not changed in any way when recording a concern; avoid asking leading questions.
- A calm and non-judgemental approach is key, particularly if it is about a sensitive issue.

If you are concerned about the behaviour of a colleague online, follow your allegations procedures and report and record to your DSL or your manager. If you are unhappy with the response you receive, follow your settings whistleblowing policy. You can also contact the NSPCC whistleblowing helpline.

10. Where else can I get information about keeping myself safe online?

The first point of contact will be to speak with your DSL and/or manager and discuss the setting's policies and procedures. If you are a member of a professional union, they may also have additional advice regarding online safety.

You may find that local support is provided to staff working in early years settings, such as via your local authority.

A glossary of terms associated with online safety can be found in the Education for a Connected World Framework.

National organisations which provide advice to professionals working with children include:

- Childnet
- London Grid for Learning
- NCA-CEOP www.thinkuknow.co.uk and www.ceop.police.uk/Safety-Centre
- UK Safer Internet Centre

This document has been bought to you by the UKCIS Education Working Group.