An e-Safety and Social Media Toolkit
For Early Years Settings

Early Years Services | August 2014 | Version 1.0
Contents

1.0 Introduction – Who is the Toolkit for?

2.0 e-Safety Policy
   2.1 Aim
   2.2 Settings Social Media Policy and Procedures
   2.3 Administration and Monitoring
   2.4 Ethical Considerations
   2.5 Out of School Clubs and Childminders

3.0 Acceptable Use Policy (AUP)

4.0 Exemplars
   4.1 Appendix 1 – Practitioner e-Safety Acceptable Use Agreement
   4.2 Appendix 2 – e-Safety Parental Permission Form
   4.3 Appendix 3 – Early Years Practitioners Conduct Agreement
   4.4 Appendix 4 – Settings Social Media Conduct Agreement
   4.5 Appendix 5 – Online Incident Log Sheet
   4.6 Appendix 6 – e-Safety Audit

5.0 Website References and Contacts for e-Safety and Social Media
1.0 Who is the toolkit for?

The toolkit is designed to be used by any setting providing services for the early years age group (birth – 5 years); however as good practice it can be applied to any organisation working with children.

The toolkit will aim to provide guidance on best practice for managing the risks associated with e-safety through policies and procedures and includes exemplars. However, early years settings will be required to tailor the policies and exemplars to meet their own individual requirements. If settings are using social networking sites e.g. Facebook and Twitter to promote their business, the registered person / safeguarding designated officer for the setting needs to be aware of and adhere to the safeguarding protocols associated with these sites.

It should be viewed as essential that parents and carers are fully involved in promoting online safety in the setting and at home. It will be beneficial to regularly consult with and discuss online safety issues with parents and carers with an aim to encourage a better understanding of the benefits and risks associated with ICT.

ICT is considered an essential life skill, and will significantly contribute to children’s enjoyment of learning and their development. In early years it is not normally expected that children would be accessing social media, however practitioners should be aware of age restrictions for each social media site used.

‘e-safety could be described as a settings ability to protect and educate children and staff in their use of information communication technology (ICT) with appropriate, effective systems in place to intervene and support with any incident (Ofsted document Inspecting e-safety reference number 120196, April 2014).

Legislation

Settings are advised to risk assess social media tools to comply with The Health & Safety at Work Act 1974, The Children Act 1989, The Childcare Act 2006, The Management of Health and Safety at Work Regulations 1999 and The Computer Misuse Act 1990 which clarify that all settings have a duty of care to ensure the safety and wellbeing of children and early years staff.

The Statutory Framework for the Early Years Foundation Stage pg.17, 3.6 states; ‘training made available by the provider must enable staff to identify signs of possible abuse and neglect at the earliest opportunity and to respond in a timely and appropriate way. Providers must train all staff to understand their safeguarding policy and procedures which should include inappropriate behaviour displayed by other members of staff which includes the inappropriate sharing of images’.
2.0 e-Safety Policy

2.1 Aim

To ensure early years practitioners have a clear and agreed understanding of the benefits and risks of e-safety. It will provide advice on acceptable use and effective control measures to enable individuals to use ICT resources in a safe online environment.

- Safeguarding children is everyone’s responsibility so it is of paramount importance to ensure the safety and wellbeing of children at all times and this includes their online safety.

- The registered person will have the overall legal, personal and moral responsibility to ensure that online safety is effectively considered.

- The designated person for safeguarding is to be responsible for online safety alongside the administrator for social media, and will manage the implementation, monitoring and reviewing of the e-safety policy.

- To minimise any risks all staff should have effective training on e-safety. A reliable infrastructure and a clear Acceptable Use Agreement (AUA) should be in place which is key to effective practice (Appendix 1).

- Creating a safer online environment will be on-going, so clear monitoring, evaluation and review of procedures are essential.

- Early years practitioners should support children’s emerging understanding of e-safety by providing a range of resources to support their learning including cameras, ipads, tablets, computers and any other android devices.

- Practitioners should be committed to acknowledge and assess risks to create a balanced approach. Relevant documentation such as incident logs (Appendix 5) and written risk assessments must be completed in accordance with the Acceptable Use Policy (AUP).

2.2 Setting’s Social Media Policy and Procedure

Social media tools can provide excellent opportunities for teaching and learning, however such sites can have risks and can never be 100% safe. These risks can be minimised by having an embedded e-safety policy and individuals should consider having separate personal and business on-line communication tools.
2.3 Administration & Monitoring

Practitioners must be aware of their personal and professional conduct when using social media. Practitioners using social media should consider what information is published to ensure confidentiality is observed at all times and the setting is not brought into disrepute. Content can be easily shared online and circulated far and wide without consent or knowledge, possibly resulting in disciplinary, civil or criminal consequences.

Points to consider

- Creating business account pages, profiles, pages or groups
- Creating a Setting’s Social Media Acceptable Use Policy (SSMAUP)
- Ensuring users of the communication tool sign a Setting’s Social Media Acceptable Use Agreement (SSMAUA)
- Creating an account using the setting’s email address and contact details
- Completing a risk assessment for use of social media
- Staff having an awareness of how sites work and their different security settings and functions
- Piloting the communication tool (social networking sites) to ensure safety and suitability
- Designating a named practitioner who is knowledgeable to administer and monitor the account
- Promoting positive use of new and emerging technologies
- Involving parents and carers in developing and reviewing the SSMAUP

2.4 Ethical Considerations

As a communication tool user you should consider the potential associated dangers of posting images, photographs and information on social networking sites. Key safety concerns include:

- Children being easily identified by their image posing a risk of inappropriate contact by individuals (children’s names must not be displayed alongside their images)
- Images being altered and distorted
- Images being used inappropriately causing stress and anxiety
All individuals regardless of age should have a right to participate in the decision making of how information is used and published. The views of children must be considered to comply with 'United Nations Convention on the Rights of the Child':

- **Article 3: Best interests of the child**

- **Article 12: Respect for the views of the child**

- **Article 13: Freedom of expression**

- **Article 16: Right to privacy**

For further information regarding the law refer to Staffordshire Safeguarding Children Board website: [www.staffsscb.org.uk](http://www.staffsscb.org.uk)

The potential risks and use considerations need to be balanced alongside the many benefits of sharing information electronically. These include parents more readily accessing information regarding the setting that their child attends and children being excited about seeing photographs of themselves displayed on the web, bringing the page to life.

### 2.5 Out of School Clubs and Childminders

Out of School Clubs and Childminders should also have regard to this additional e-safety guidance.

- Do not give away any personal or private information. If you set up a webpage advertising your business do not give out lots of detail about yourself or the children you are looking after. For example do not state your daily routine in which you include specific times when you are out of the house.

- Check your privacy settings to ensure only people you know and trust see your full profile.

- Do not share contact lists as details could get passed on without your consent.

- Consider the photographs you post, check you have parental permission or use stock photographs to minimise the risks of children being identified.

- Think about the messages you send to ensure that they are appropriate.

- Review your anti bullying policy to ensure it covers electronic bullying and consider asking older children to sign an e-safety agreement (see [www.safenetwork.org.uk](http://www.safenetwork.org.uk) for further information).

- If a child reports something to you which makes them feel scared or worried, report this concern to the police or use the report abuse button on the Child Exploitation Online Protection agency, (CEOP), website [www.thinkyouknow.co.uk](http://www.thinkyouknow.co.uk).

- Consider children’s access to devices that provide internet access for example Xbox and Play Station and ensure that filters are set to high security.

- Do not allow access to networking sites via your system.
Electronically held personal information must be stored securely and within the guidelines of
the Information Commissioners Office (ICO) [www.ico.gov.uk](http://www.ico.gov.uk). If information is taken off site
e.g. laptops or data sticks, then this process must be risk assessed and have the
permission of the line manager.

For further information refer to Staffordshire Safeguarding Children Board website: -
[www.staffsscb.org.uk](http://www.staffsscb.org.uk)
3.0 Acceptable Use Policy (AUP)

Aim

AUP gives users a clear understanding of what they can and cannot do, how their use will be monitored and the sanctions for misuse. AUP will apply to all individuals, with the registered person having overall responsibility for ensuring that online safety is implemented as part of everyday safeguarding practice. Clear, robust policies and procedures, including allegations of misuse, should be available.

- All practitioners should receive appropriate training, guidance, time and resources to implement the policies and procedures.

- AUP should outline the responsibilities of all individuals who have access to and use of ICT systems and ensure that everyone has a clear understanding of what constitutes misuse and the sanctions that may be applied.

- Individuals will be provided with a copy of the AUP and be expected to sign the Acceptable Use Agreement (AUA), a copy of which will be kept on file (Appendix 1).

- The appropriately trained designated safeguarding person/manager and/or named e-safety administrator should be responsible for ensuring all aspects of online safety are implemented including openly monitoring and regularly reviewing the AUP.

- Any inappropriate behaviour/actions will be taken seriously and in the event of an allegation of misuse, the designated e-safety administrator must inform the setting safeguarding officer who will contact the police if it is a criminal matter or First Response if it is a safeguarding or welfare concern. They may also need to report any concerns about misuse or incidents to CEOP.

- The AUP should be clearly linked to the e-safety policy or camera/mobile phone policy.

- All individuals will be expected to write online communications in a professional manner and it will be considered inappropriate for early years practitioners to engage in personal online communications with children, parents or carers. Refer to ‘Guidance for Safer Working Practice for Adults who Work with Children’ (2013).
  webarchive.nationalarchives.gov.uk/...everychildmatters/...practice/ig00

- Childcare practitioners should not have personal communication, including on social network sites, with the children, parents and carers with whom they act in a professional capacity. There may be occasions when the practitioner and the adults in the family are friends prior to the child coming into the setting. This information should be shared with the manager, or in the case of childminders, risk assessed and appropriate boundaries for safeguarding the children and the practitioner agreed.

- Practitioners must sign the Professional Conduct Agreement (Appendix 3).
• Parents need to be consulted and must provide written agreement for their children to access online resources which will also be monitored by a supervising adult (Appendix 2: e-Safety Parental Permission Form).

• Any devices equipped with internet access should be considered subject to the same risks as any other form of technology.

• Strong passwords (combination of numbers, symbols and lower/upper case letters) are essential, must be kept secure and be regularly updated.

• A time out should be set on all computers if they become idle for a period of time. All users must log out of their accounts should they need to leave a computer unattended.

• To assess and minimise risk consider:
  • having secure password systems for broadband, wireless connection, email account and websites.
  • ensuring your virus protection is checked regularly, updated and is fit for purpose (includes internet filtering).
  • having an agreed list of assigned authorised users with controlled access.

• Complete an effective e-safety audit (Appendix 6).

• Place computers and gaming machines in areas of high visibility.
4.0 Exemplars

4.1 Appendix 1

Practitioner e-Safety Acceptable Use Agreement

In order to support your practice in developing the children’s knowledge and understanding about e-safety, please read and agree to the following information.

e-Safety acceptable use agreement return form

- I understand, accept and agree to adhere to (name of setting) e-safety policy;
- I understand it is my responsibility to ensure safe and responsible use of ICT within (name of setting);
- I understand that (name of setting) ICT systems are primarily intended for educational use and that I will only use the systems for personal and recreational use within the policies and rules set down by the setting;
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person;
- I will only use chat and social networking sites in accordance with the setting’s policies;
- I will not engage in any online activities that may compromise my professional responsibilities;
- I will only communicate with parents, carers and other professionals using official systems. Any such communication must be professional in tone and manner;
- If I fail to comply with this AUA I could be subject to disciplinary action.

I have read and understood the above and agree to use (name of setting).systems, both in and out of the setting, and my own devices, within these guidelines.

Practitioner’s name: _____________________________

Signature: __________________________

Date: ___/___/___


4.2 Appendix 2

e-Safety Parental Permission Form

Dear Parent/Carer

As part of the programme of activities to support your child’s learning and development, they will have the opportunity to access a wide range of information and communication technology (ICT) resources.

We recognise the important contribution and value that such resources have in promoting children’s learning and development, however, we also recognise there are potential risks involved and therefore have robust e-safety policies and procedures in place.

- Please read and sign the permission form below.

Should you wish to discuss the matter further please do not hesitate to contact me.

Yours sincerely,

(Manager)

----------------------------------------------------------------------------------------------------

Parent/Carer e-Safety Permission Form

I give permission for my child to access digital technologies in accordance with (name of setting) e-safety policies and procedures.

Child’s Name: _______________________________

Parent/Carer Name: _________________________

Parent/Carer Signature: _____________________ (person with parental responsibility)

Date: ___/___/___
4.3 Appendix 3

Early Years Practitioners Conduct Agreement

We acknowledge that practitioners will use digital technologies in their personal and social lives so we require them to sign the following Professional Conduct Agreement to ensure clear boundaries between their home and professional roles.

I agree that through my recreational use of social networking sites or other online technologies that I will:

- not bring *(name of setting)* into disrepute;
- observe confidentiality and refrain from discussing any issues relating to work;
- not share or post in an open forum, any information that I would not want children, parents/carers or colleagues to view;
- set privacy settings to block unauthorised access to my social networking page and to restrict those who are able to receive updates;
- keep my professional and personal life separate and not accept children and parents/carers as ‘friends’;
- consider how my social conduct may be perceived by others and how this could affect my own reputation and that of the *(name of setting)*;
- either avoid using a profile photograph or ensure it is an image I would be happy to share with anyone;
- report any known breaches of the above;
- I understand I am in a position of trust and my actions outside of my professional environment could be misinterpreted by others, and I am conscious of this when sharing information publicly with others.

Name: ________________________          Signature: ________________________
Date: ___/___/___
4.4 Appendix 4

Setting’s Social Media Conduct Agreement

We require you to sign and agree to follow the Conduct Agreement for using (name of setting) social media communication platforms to ensure clear boundaries between (name of setting) and home are followed.

Social Media Platform: ___________________________

I agree to:

- Follow their social media policy and not bring (name of setting) into disrepute;
- observe confidentiality by not discussing other children, parents or practitioners;
- not share, tag, post or copy any information from (setting name) social media platform without prior permission from the ‘management’;
- keep my professional and personal life separate and not accept children/parents/carers as ‘friends’ on my personal page;
- consider how my social conduct may be perceived by others and how this could affect my own reputation and that of (name of setting);
- report any known breaches of the above to the designated person for safeguarding (name of person) and named social media administrator (name of person) for social media;
- I understand I am in a position of trust and my actions could be misinterpreted by others and I am conscious of this when sharing information with others on the social media platform site belonging to (name of setting).

Name : ______________________          Signature: ________________

Date: ____/____/_____
4.5 Appendix 5

Online Incident Log Sheet

An e-safety flow chart to assist you in determining the process to follow in the event of an e-safety incident refer to www.safenetwork.org.uk

To be completed as thoroughly as possible by the practitioner or manager identifying incident

Date(s) / time(s) of incident:

Duration of incident: (e.g. one off, a week)

Description of the online safety incident (include details of specific services or websites used e.g. chat room, email addresses, usernames etc.

Why do you have concerns about this incident?

Has the information been recorded and secured? Yes/ No
Has any computer or hardware been secured? Yes/ No

If yes, give details including who, where, when and what?

Who was involved and how do you know this?

Is there any evidence to suggest that false names/details have been given? (Give full details of real names and email addresses where known).
How was the incident identified? e.g. by member of staff

What actions were taken, by whom and why? (Give detail of agencies informed and contact person within those agencies).

Name of person completing this form:

Position:

Name of setting:

Signature:

Date:
### 4.6 Appendix 6

**e-Safety Audit**

This self audit should be completed by the manager, the designated person for safeguarding and the designated person for monitoring any online communication tools. Staff, parents and carers could also contribute to this audit tool.

<table>
<thead>
<tr>
<th>Task</th>
<th>Yes/No</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the e-safety policy comply with local safeguarding children board's e-safety procedures and guidance?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is e-safety included in the induction process for all new staff?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has up to date training been provided for all individuals?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all individuals (early years practitioners, parents, carers and any volunteers) familiar with the e-safety policy and the Acceptable Use Policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have early years practitioners and any volunteers (including parents / carers if applicable) signed a disclaimer to say they have read and understand the e-safety Policy and the Acceptable Use Policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have parents/carers returned and signed a copy of the e-safety parental permission form?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Yes/No</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>All individuals are compliant with additional AUP’s (social media sites, learning platforms) and have signed the additional disclaimer for their use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do users understand the use of e-safety monitoring software (if applicable)?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did you consult early years practitioners, parents/carers when updating the e-safety policy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all individuals made aware of the settings expectation around safe and professional online behaviour?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a clear procedure for all individuals to follow when responding or reporting an e-safety incident or concern?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is personal data collected, stored and used in accordance with the principles of the Data Protection Act and ICO?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you accessed and distributed e-safety materials from SSCB, CEOP, Childnet and UKCCIS?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you devised an e-safety and social media incident log that is used to record incidents and any action taken?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have you devised e-safety and social media rules? How are these communicated to individuals?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.0 References and Contacts for e-Safety and Social Media

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Connect Safely: http://www.connectsafely.org/
Cybermentors: www.cybermentors.org.uk
Digizen: http://www.digizen.org/
Facebook Safety Centre: https://en-gb.facebook.com/safety/
Information Commissioner's Office - Data Protection: http://www.ico.org.uk/for_organisations/data_protection
Internet Watch Foundation (IWF): www.iwf.org.uk
Kent e–Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety
Kidsmart: www.kidsmart.org.uk
Safe Network- http://www.safenetwork.org.uk/
Staffordshire Safeguarding Children Board: http://www.staffsscb.org.uk
South West Grid for Learning Online Safety: http://www.swgfl.org.uk/Staying-Safe
Teach Today: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Twitter- Safety Tips for Parents: http://support.twitter.com/articles/470968-safety-tips-for-parents#
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com
Wired Safety - https://www.wiredsafety.org
Disclaimer

Entrust Early Years Services attempts to ensure that the information in this document is accurate and up to date.

Entrust Early Years Services and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication.