

E-safety:

Guidance and toolkit for schools, colleges and other settings  
working with Children and Young People in Dudley



## **Introduction**

Rapid developments in technology and online behaviour present excellent opportunities but also new risks to children and young people such as online abuse, exploitation, exposure to explicit material, grooming, radicalisation and cyberbullying.

Dudley's E-safety Task Group is a subgroup of Dudley Safeguarding Children Board. It is a multi-agency group of practitioners working with / for young people across the borough to ensure that we, as a partnership, are doing as much as we can to ensure that our children and young people are kept safe from online risks and abuse through the 'E-safety Strategy' and Action plan

Dudley's E-safety strategy is built on four key strands: educate and inform; safety; safeguarding; monitoring, evaluation and review.

These activities take place in communities and other places across the borough where the internet and other technologies are used. This includes formal and informal settings such as schools, colleges, alternative education provision, child care and youth centres, among others.

This toolkit has been created in order to signpost practitioners working with children and young people across the borough to recommended resources, policies and guidance in relation to E-safety.

The intention is that schools and settings can use the information in this toolkit to look at both legal requirements and E-safety best practice, with a view to refreshing their own documents to reflect the practices of their school/settings.

For schools and other educational settings this is an opportunity to ensure that all documents are up to date, ready for the start of the following academic year.

We are launching this toolkit to coincide with National Safer Internet Day, which takes place every year on 10<sup>th</sup> February<sup>1</sup>.

---

<sup>1</sup> <http://www.saferinternet.org.uk/safer-internet-day/2015>

## What do we mean by E-safety?

E-safety is the safe and responsible use of technology - not just the internet but of mobile phones and other devices. It also includes our responsibilities to other users to ensure that we are not making them feel scared or unsafe or encouraging them to break the law in any way.

## Young people and E-Safety

Ongoing research is taking place nationally and in Dudley through the 'cyber survey'. This was last undertaken in 2013<sup>2</sup>. We know that children and young people are, on the whole, receiving good quality advice, but we also know that they do not always follow this advice.

**Top Tips from young people** (many thanks to students from Holly Hall Academy):

*For young people:*

- Don't add people you don't know to Facebook / Twitter / Instagram etc unless you know them
- Check your privacy settings on social networking sites – think - who can see your info?
- Never give out ANY personal details online
- If you are being 'cyber bullied' keep all the evidence and tell a trusted adult or use the report it button
- Block anybody who sends you stuff you don't like
- Don't reply to abusive messages / emails
- Regularly check your friends lists to make sure you know everyone in it - delete anyone you don't know
- If anything makes you feel scared or uncomfortable while you are online tell a trusted adult or use the report it button
- Think before you send a message – they can sometimes be taken the wrong way
- NEVER meet someone that you have only met online
- Always think twice before putting your picture online, people can copy it, edit it and use it for other things

*For parents*

- Respect your children's privacy – do not 'snoop' in their phone / websites
- Watch out for any changes in your child. If you see any, share your concerns with the school to see if they have noticed anything
- 'Clean' your child's friend list **with** them

---

<sup>2</sup> Contact [Lynda.kesterton@dudley.gov.uk](mailto:Lynda.kesterton@dudley.gov.uk) for more information about the cybersurvey

- If your child is being bullied, support them – don't punish them by taking away their mobile / internet access – it's not their fault
- Show an interest – find out what websites they are going on
- Tell them to keep pass words and personal details safe
- Get a good firewall and use parental blocks where appropriate
- Tell them to show you any messages they don't like
- Help them feel comfortable talking to you – make sure they know they can talk to you about anything
- Tell them where else they can go if they don't feel comfortable talking to you about stuff (report button / childline etc)
- Remember they can access the internet through loads of devices including games consoles

**Recommended websites for information and resources:**

<i>For practitioners:</i>	<i>For children and young people:</i>	<i>For parents:</i>
<a href="http://www.thinkuknow.co.uk">www.thinkuknow.co.uk</a>	<a href="http://www.thinkuknow.co.uk">www.thinkuknow.co.uk</a>	<a href="http://www.thinkuknow.co.uk">www.thinkuknow.co.uk</a>
<a href="http://www.saferinternet.org.uk/">http://www.saferinternet.org.uk/</a>	<a href="http://www.chatdanger.com">www.chatdanger.com</a>	<a href="http://www.childnet.com/parents-and-carers">http://www.childnet.com/parents-and-carers</a>
<a href="http://www.internetmatters.org">http://www.internetmatters.org</a>	<a href="http://www.internetmatters.org">http://www.internetmatters.org</a>	<a href="http://www.internetmatters.org">http://www.internetmatters.org</a>
<a href="http://www.dudley.rmplc.co.uk/12/13/tz_s_s.shtm">http://www.dudley.rmplc.co.uk/12/13/tz_s_s.shtm</a> (access on DGfL and DMBC networks only)	<a href="http://www.digizen.org/kids/">http://www.digizen.org/kids/</a>	<a href="http://www.digizen.org/parents/">http://www.digizen.org/parents/</a>
<a href="http://www.childnet.com/teachers-and-professionals">http://www.childnet.com/teachers-and-professionals</a>	<a href="http://www.childnet.com/young-people">http://www.childnet.com/young-people</a>	<a href="http://www.netlingo.com/acronyms.php">http://www.netlingo.com/acronyms.php</a>
<a href="http://www.swgfl.org.uk/products-services/Online-Safety-Services">http://www.swgfl.org.uk/products-services/Online-Safety-Services</a>	<a href="http://www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx">http://www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx</a>	
<a href="http://www.digizen.org/teachers/">http://www.digizen.org/teachers/</a>		
<a href="http://www.netlingo.com/acronyms.php">http://www.netlingo.com/acronyms.php</a>		

### Ofsted - Key features of good and outstanding practice<sup>3</sup>

<p>Whole school consistent approach</p>	<p>All teaching and non-teaching staff can recognise and are aware of e-safety issues.</p> <p>High quality leadership and management make e-safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-Safety Mark).</p> <p>A high priority given to training in e-safety, extending expertise widely and building internal capacity.</p> <p>The contribution of pupils, parents and the wider school community is valued and integrated.</p>
<p>Robust and integrated reporting routines</p>	<p>School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems.</p> <p>Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.</p>
<p>Staff</p>	<p>All teaching and non-teaching staff receive regular and up-to-date training.</p> <p>One or more members of staff have a higher level of expertise and clearly defined responsibilities.</p>
<p>Policies</p>	<p>Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors.</p> <p>The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying.</p> <p>The e-safety policy should incorporate an Acceptable Usage Policy that is understood and respected by pupils, staff and parents.</p>
<p>Education</p>	<p>An age-appropriate e-safety curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.</p> <p>Positive rewards are used to cultivate positive and responsible use.</p> <p>Peer mentoring programmes.</p>
<p>Infrastructure</p>	<p>Recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored.</p>
<p>Monitoring and Evaluation</p>	<p>Risk assessment taken seriously and used to good effect in promoting e-safety.</p> <p>Using data effectively to assess the impact of e-safety practice and how this informs strategy.</p>
<p>Management of Personal Data</p>	<p>The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.</p> <p>Any professional communications between the setting and clients that utilise technology should:</p> <ul style="list-style-type: none"> <li>• take place within clear and explicit professional boundaries</li> <li>• be transparent and open to scrutiny</li> <li>• not share any personal information with a child or young person.</li> </ul>

<sup>3</sup> Inspecting E-safety, January 2013, No 120196

## E-safety Checklist

<b>Policy</b>		
<i>Schools</i>	<i>DMBC</i>	<i>Other settings</i>
<a href="#">E safety policy template</a>	<a href="#">E safety policy</a>	<a href="#">E safety policy</a>
<a href="#">Staff and pupils AUP</a> (contained in E-safety policy)	<a href="#">Corporate AUP</a>	Acceptable Use Policy
<a href="#">Community users AUP's</a> (contained in E-safety policy)	<a href="#">Social Media Policy</a>	Social Media Policy
<a href="#">Information governance for schools</a> (access requests through Sharron Andrews: <a href="mailto:sharron.andrews@dudley.gov.uk">sharron.andrews@dudley.gov.uk</a> )	<a href="#">Corporate information Governance</a> (Information Security, Freedom of Information, Data Protection)	Information Governance (Information Security, Freedom of Information, Data Protection)
	<a href="#">Code of conduct</a> (includes a section on social networking)	
<b>Guidance</b>		
<i>Schools</i>	<i>DMBC</i>	<i>Other settings</i>
<a href="#">Ofsted Inspecting - E-safety, January 2014, No 120196</a>	<a href="#">Ofsted Inspecting E-safety, January 2014, No 120196</a>	<a href="#">Ofsted Inspecting E-safety, January 2014, No 120196</a>
<a href="#">DSCB use of images</a> NB it is advisory to check consent annually due to possible change in circumstances	<a href="#">DSCB use of images</a> NB it is advisory to check consent annually due to possible change in circumstances	<a href="#">DSCB use of images</a> NB it is advisory to check consent annually due to possible change in circumstances
<a href="#">DSCB Child Abuse and New Technologies</a>	<a href="#">DSCB Child Abuse and New Technologies</a>	<a href="#">DSCB Child Abuse and New Technologies</a>
<a href="#">DSCB social networking guidance – safeguarding children, young people and vulnerable adults</a>	<a href="#">DSCB social networking guidance – safeguarding children, young people and vulnerable adults</a>	<a href="#">DSCB social networking guidance – safeguarding children, young people and vulnerable adults</a>
<a href="#">DSCB social networking guidance – safeguarding yourself</a>	<a href="#">DSCB social networking guidance – safeguarding yourself</a>	<a href="#">DSCB social networking guidance – safeguarding yourself</a>
<a href="#">DSCB social networking guidance – safeguarding your organisation</a>	<a href="#">DSCB social networking guidance – safeguarding your organisation</a>	<a href="#">DSCB social networking guidance – safeguarding your organisation</a>
<a href="#">Resources for staff</a> (access on DGfL and DMBC networks only)	<a href="#">Resources for staff</a> (access on DGfL and DMBC networks only)	
<a href="#">Resources to be used with learners</a> (access on DGfL and DMBC networks only)	<a href="#">Resources to be used with learners</a> (access on DGfL and DMBC networks only)	

## **Where to report**

<b>CEOP</b>	<a href="http://ceop.police.uk/">http://ceop.police.uk/</a>
<b>Internet Watch Foundation</b>	<a href="https://www.iwf.org.uk/">https://www.iwf.org.uk/</a>
<b>Childline</b>	<a href="http://www.childline.org.uk/pages/home.aspx">http://www.childline.org.uk/pages/home.aspx</a>
<b>West Midlands Police</b>	101 (999 in an emergency)
<b>Anti-terrorist Hotline</b>	0800 789 321
<b>Social Care Offices</b>	Dudley 01384 813200 Brierley Hill 01384 813000 Halesowen/Stourbridge 01384 815902
<b>Emergency Duty Team</b>	Dudley - Out of hours 0300 555 8574
<b>Education safeguarding</b>	Funbir Jaspal: <a href="mailto:funbir.jaspal@dudley.gov.uk">funbir.jaspal@dudley.gov.uk</a>

## **Other useful contacts:**

<b>Anti-bullying Coordinator</b>	Lynda Kesterton: <a href="mailto:Lynda.Kesterton@dudley.gov.uk">Lynda.Kesterton@dudley.gov.uk</a>
<b>Dudley Grid for learning</b>	Heather Jeavons: <a href="mailto:hjeavons@dgfl.org">hjeavons@dgfl.org</a>
<b>Child Sexual Exploitation</b>	Helen Matthews: <a href="mailto:helen.matthews@street-teams.org">helen.matthews@street-teams.org</a>
<b>Preventing Violent Extremism</b>	P.C. 4146 Eamonn Hall: <a href="mailto:e.hall@west-midlands.pnn.police.uk">e.hall@west-midlands.pnn.police.uk</a>

For details of training: <http://safeguarding.dudley.gov.uk/child/work-with-children-young-people/>