E-safety:

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

DGfL3

Dudley Safeguarding
protecting children and young people

safe & sound
Dudley's Community Safety Partnership

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 10th February[1].

[1] 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[2]. 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

[2] Contact 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:

For practitioners:	***For children and young people:***	***For parents:***
www.thinkuknow.co.uk	www.thinkuknow.co.uk	www.thinkuknow.co.uk
http://www.saferinternet.org.uk/	www.chatdanger.com	http://www.childnet.com/parents-and-carers
http://www.internetmatters.org	http://www.internetmatters.org	http://www.internetmatters.org
http://www.dudley.rmplc.co.uk/l2/l3/tz_s_s.shtm (access on DGfL and DMBC networks only)	http://www.digizen.org/kids/	http://www.digizen.org/parents/
http://www.childnet.com/teachers-and-professionals	http://www.childnet.com/young-people	http://www.netlingo.com/acronyms.php
http://www.swgfl.org.uk/products-services/Online-Safety-Services	http://www.childline.org.uk/Explore/OnlineSafety/Pages/OnlineSafety.aspx	
http://www.digizen.org/teachers/		
http://www.netlingo.com/acronyms.php		

Ofsted - Key features of good and outstanding practice[3]

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e-safety issues. 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). A high priority given to training in e-safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based reporting routes that are clearly understood and used by the whole school, for example online anonymous reporting systems. Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. One or more members of staff have a higher level of expertise and clearly defined responsibilities.
Policies	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. The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The e-safety policy should incorporate an Acceptable Usage Policy that is understood and respected by pupils, staff and parents.
Education	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. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider (ISP) or Regional Broadband Consortium (RBC) together with age-related filtering that is actively monitored.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-safety. Using data effectively to assess the impact of e-safety practice and how this informs strategy.
Management of Personal Data	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. Any professional communications between the setting and clients that utilise technology should: • take place within clear and explicit professional boundaries • be transparent and open to scrutiny • not share any personal information with a child or young person.

[3] Inspecting E-safety, January 2013, No 120196

E-safety Checklist

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

Where to report

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

Other useful contacts:

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

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