

Online Safety Newsletter

July 2016



Contents

- 1 Introduction
Keeping children safe in education
- 2 Definitions about appropriate filtering and monitoring
Filtering and monitoring in South Gloucestershire
Educate against hate website
- 3 Trust me resource on online extremism
Increase in sexting in schools
Managing sexting incidents
- 4 Enable resources against bullying
Data protection and information security self-evaluation tool – 360 data
CyberSense app for parents and carers
Net aware resources from NSPCC
- 5 Think U Know parents and carers campaign
UKCCIS parent's guide
- 6 CPD update
Contact details

Introduction

Welcome to our online safety newsletter. We gather information from a wide variety of sources to provide a regular update.

Keeping children safe in education

This statutory guidance document has been updated and the revised version is due to come into force in September. It can be accessed at the link below.

[Keeping Children Safe in Education Document](#)

The new document provides additional expectations about online safety. The references are detailed here.

Page 11 of the document mentions abuse online via the internet as a type of abuse. Cyberbullying is mentioned linked to emotional abuse. The sexual abuse section includes mention of non-contact activities via the internet such as grooming and production of sexual images.

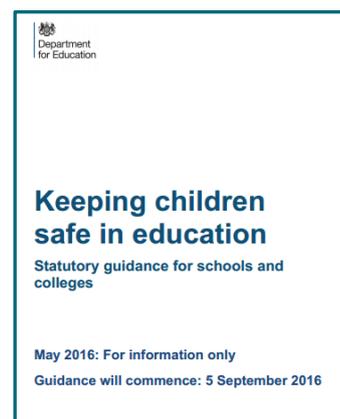
Page 12 under specific safeguarding issues identifies the need for staff to be aware of sexting as a behaviour that could put children in danger. Cyberbullying is also emphasised.

On page 14 in the management of safeguarding section the need is highlighted for governing boards to ensure that there are appropriate policies and procedures in place such as a staff behaviour policy which should include acceptable use of technologies, staff/pupil relationships and communications including the use of social media.

Page 17 includes sections about online safety and teaching opportunities and the text is reproduced below.

Online safety

As schools and colleges increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional



information to support governing bodies and proprietors is provided in Annex C.

Opportunities to teach safeguarding

Governing bodies and proprietors should ensure children are taught about safeguarding, including online, through teaching and learning opportunities, providing a broad and balanced curriculum.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place; they should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Page 54 and 55 outline information on preventing radicalisation which includes references to online influences.

Page 56 states that:

Schools must ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

The document has prompted debate as to what constitutes appropriate filtering and monitoring.

Definitions about appropriate filtering and monitoring

Safer Internet Centre have put together some definitions and guidance for schools and providers.

[Appropriate filtering and monitoring guidance](#)

Filtering for South Gloucestershire Primary Schools

Working together, staff from Schools IT and the Curriculum Team, have reviewed the current filtering solution for schools to identify whether we feel it fulfils the expectations in Keeping Children Safe in Education. We have identified a number of key areas where this might not be providing the level of robust support that is required to ensure that young people are safeguarded. This includes having appropriate filtering to prevent radicalisation using the latest DfE list.

You will have received a letter from Andreas Burt about this. The solution we are proposing is in addition to your current filtering and will provide enhancements that support the new requirements. These enhancements are:

- active monitoring and automatic alerts for the school to act upon, together with pro-active

monitoring by Integra Schools IT - this will support schools by drawing attention to concerning behaviours, communications or access

- age appropriate filtering and monitoring
- enhanced filtering integrating with the police assessed list of unlawful terrorist content, produced on behalf of the home office
- delegated access allowing you to control the filtering yourselves to permit or deny access to specific content
- network level filtering which does not rely on any software on the users devices which could be disabled
- ability to produce reports on the websites visited by your users
- the ability for alerts to be set so that a number of people are informed when they are triggered - this means that monitoring does not need to fall into the remit of one person
- the ability to have external alerts to people outside the school (such as safeguarding, online safety or IT technicians) so that **monitoring is not only reliant on school staff**
- staff will have early indication of young people accessing content that could make them vulnerable and therefore be able to take appropriate action in line with Prevent to safeguard them
- automates the reporting process to ensure that action is always taken in response to an issue
- for governors, the added safeguard of ensuring reporting **does not just rely on internal staff**

We have currently asked schools to signal their interest in this and will be providing further information. Please contact Andreas Burt at Andreas.burt@southglos.gov.uk if you have queries about this.

The logo for 'educate.against.hate' features the words 'educate.against.hate' in a bold, sans-serif font. The word 'hate' is written in a smaller font size and is crossed out by a thick red horizontal line.

[The DfE has announced the launch](#) of a new website called '[Educate against hate](#)'. This is designed to offer practical advice and information for parents, teachers and school leaders about extremism and radicalisation. It has been created with consultation from organisations such as Childnet and the UK Safer Internet Centre, and it will include information on:

- warning signs of danger,
- how parents should talk to children about extremism and
- steps concerned parents can take.

The website contains advice regarding preventing all forms of extremism, including, for example, far-right views. It contains links to relevant guidance and resources to enable teachers and school leaders to ensure they are taking all required steps to safeguarding their community.

For teachers there are links to topics like:

- Why is extremism relevant?
- How do people become radicalised?
- Which children and young people may be vulnerable?
- What are the warning signs?
- What should I be teaching?

For parents there are topics such as:

- How to protect my child
- How to talk to my child about the issues
- What parents should know about the online risks

UK Safer Internet Centre are also developing teaching resources to support schools open a dialogue with young people and parents.

[Educate against hate website](#)

Trust me – PSHE Resource on Online Extremism

On 19 May 2016, Childnet launched a new KS2 and KS3 PSHE resource called "Trust me". This is a practical resource which is aimed at challenging young people to think critically about what they see online. It has been created as a response to online extremism.

Young people's views of the world are increasingly coloured by media reporting so it is important we give them the skills to critically assess and analyse the information they are exposed to. The Trust me resource is aimed at encouraging young people to think more critically about what they see online.



The resource includes mocked-up examples of social media posts and websites that young people can critically assess. There are practical activities and discussion guides for teachers to follow. There are primary and secondary packs and each pack contains:

- A lesson plan relating to online **content** (*can you believe everything you read online?*)
- A lesson plan relating to online **contact** (*can you trust everyone you speak to online?*)
- A lesson plan relating to **propaganda** and media literacy (*only in secondary pack*)

Lesson plans are intended to provoke discussion and to allow young people to reflect on the motives and agendas behind what we see online and who we speak to online. Resources explore questions like 'how can we know if a website is trustworthy online?' and 'why and how might someone gain your trust online?'

Trust Me is free to access on the Childnet website at the link below.

<http://www.childnet.com/resources/trust-me>

Increase in sexting in schools

Senior police officers have reported an escalation in sexting offences in schools, according to a report submitted to MPs.

National Police Chiefs' Council (NPCC) warned a Commons Select Committee that sexual harassment was not always being recognised for what it was in the classroom and pupils did not understand the meaning of consent. Read the article at the link below.

[Increase in sexting offences article](#)

The escalation in sexting among children was confirmed by the National Society for the Prevention of Cruelty to Children (NSPCC) who reported a 15% increase in ChildLine counselling sessions for sexting, compared with the previous year. The "[sexting advice page](#)" is the most viewed on the ChildLine website, it said.

Managing sexting incidents in schools

Safer Internet Centre report that many schools are dealing with sexting incidents. Safer Internet Centre have produced some guidance for schools on responding to and managing these incidents. This will help to support staff with deciding when incidents



Context
With the rise of sexting incidents involving young people, this guidance aims to help schools identify sexting incidents, manage them and escalate appropriately.

For School Staff
Remember: The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

Step 1: If a device is involved - confiscate it and set it to flight mode or, if not possible, switch it off.

Step 2: Seek advice - report to your designated safeguarding lead via your normal child protection procedures.

For the Designated Safeguarding Lead
Record all incidents of sexting, including both the actions you did take as well as the actions you didn't take and give justifications. In applying judgement to each incident, consider the following:

- Is there a significant age difference between the sender/receiver involved?
- Is there any external coercion involved or encouragement beyond the sender/receiver?
- Do you recognise the child as more vulnerable than usual (i.e. at risk)?
- Is the image of a severe or extreme nature?
- Is the situation isolated or has the image been more widely distributed?
- Have these children been involved in a sexting incident before?
- Are there other circumstances relating to either sender or recipient that may add cause for concern (i.e. difficult home circumstances)?

If any of these circumstances are present, then do escalate or refer the incident using your normal child protection procedures. This includes reporting to the police.

If none of these circumstances are present, then manage the situation accordingly within the school and without escalating to external services. Record the details of the incident, action and resolution.

SWGfL UK Safer Internet Centre
Co-Produced by the Safer Internet Centre
© Crown Copyright 2016

need escalation to the police.

The resources can be accessed at the weblinks below.

[Sexting resources](#)

[Guidance document](#)

Enable Lesson Resources and Peer Support Tools

ENABLE is the European Network Against Bullying in Learning and Leisure Environments. It is an EU-funded project where partner countries are working together to combat bullying for young people aged 11-14 through social and emotional development and peer education. It involves students, staff and parents/ carers.

Benefits to implementing the programme can be:



- Supporting a positive whole-school climate
- Improving emotional awareness for both staff and students
- Higher attainment in assessments
- Reduced truancy and bullying incidents
- Improved staff well-being

The programme includes ten social and emotional learning lesson modules for schools to help explore the four areas of emotional intelligence – self-awareness, social awareness, self-management and relationship management. The second part of the programme is a planned programme for Peer Supporters.

The resources are freely available and can be downloaded from

<http://enable.eun.org>

There is a document called *Making ENABLE work* which provides guidance on implementing the programme successfully in your school.



Data Protection and Information Security

360Data has been launched. This online tool is designed to help schools and organisations review their practice, policies and procedures around data protection and information security.

Although it is a subscription service there is a free 30 second self-evaluation quiz that highlights some of the issues and can give you some high level pointers and feedback.

The information can be accessed at the link below.

[360 Data Link](#)

CyberSense App for Parents and Carers

Internet Matters have produced this app designed to help parents and carers talk about online safety issues with their children. The aim is to help them ensure that their children make smart choices to stay safe online.



It is aimed at children aged 8-10 and designed to help them think about what they would do if they were faced with different situations online. Scenarios range from [cyberbullying](#) to sharing content with someone they don't know.

There is a quiz that which is played on a tablet with a split screen where parents/carers and children can answer the questions at the same time to help create talking points around different online safety scenarios. At the end of each quiz, there is a reward of a fun game to play together which is related to the number of questions that were answered correctly.

The app can be downloaded for free on the [iTunes app store](#) and [Google Play](#) store.

Updated Net Aware Resources from NSPCC

NSPCC have re-launched their [Net Aware](#) guide. This is a simple guide to the social networks, sites and apps children use. It is based on parents' experiences and

the views of young people. Over 750 reviews from a parent panel and over 1720 young people reviewed 50 platforms against criteria such as reporting mechanisms, privacy and prevalence of inappropriate content. Their website allows parents to search for different platforms to find out about them. The website link is below.

[Net Aware Website](#)



NSPCC have also launched a Net Aware app which is available to download from iTunes and Google play.

The NSPCC hope that providing parents with up-to-date information about the sites most commonly used by young people will enable them to talk to their children about staying safe on those platforms. They also want to encourage providers to take action to make their sites as safe as possible for children.

We hope you will publicise this to parents and carers of 8-12 year olds so that we can reach as many as possible.

Please also promote the Net Aware update on your school social media platforms by tweeting using #NetAware using your professional or school accounts.

Thinkuknow resources for parents and carers

Thinkuknow want to get parents and carers thinking and talking about the importance of discussing sex, relationships and the internet with their children through social media, articles, blogs, films and more. They have developed a resource entitled **“The world changes. Children don’t”**.

This is a short film that tells the story of Romeo and Juliet with a modern twist showing how their lives might play out online today, including the Lark ‘tweeting’ and Romeo ‘friending’ Juliet.

The message behind this is that technology and social media may seem overwhelming and constantly changing however, children and young people don’t change. The resource reminds parents their children

are still exploring and creating their identities, keeping up with their friends and dealing with adolescent pressures. Much of this may now happen online but the parental support and advice which keeps their children safe ‘in real life’ will keep them safer online too. The resources can provide a useful starting point to help with these discussions.

The film can be seen at the link below.

[‘The world changes. Children don’t’ film](#)

The parents section of the Thinkuknow website provides information to support parents and carers. It helps them to understand and respond to the risks their children may face as they grow and covers a range of online safety issues from nude selfies to what to do if you think your child is being groomed online.

The website can be accessed at the link below.

www.thinkuknow.co.uk/parents.

Child Safety Online Guide for Parents

UKCCIS have developed a guide to help parents keep their children safer online. It includes information on:

- Social media
- What children could see, who they might meet and how this could affect them
- Practical tips to help minimise the risks to their child
- Ideas to support them with talking to their child
- How to make a report if they are concerned
- Links to support



[Child online safety: a practical guide for parents and carers whose children are using social media](#) (PDF)

CPD Update

Regular online safety updates are provided as part of our Primary ICT Best Practice Forum meetings. The meeting dates are below and these can be booked through CPD online.

2016 – 2017 Best Practice Dates

Computing group 1	18 October 7 February 23 May
Computing group 2	19 October 8 February 24 May

We will be offering online safety training later in the year and are planning a safeguarding conference for the Spring.

SWGfL Online Safety Briefing

As part of their e-safety live programme SWGfL will be running an online safety briefing at Little Stoke Training rooms in September.

Information will appear on their website at the link below when the date has been confirmed.

[Online safety live briefings](#)

Governor Online Safety Briefing

As part of the governor development programme we are running an online safety briefing for governors on 31 January 2017.

This can be booked through governor services and is available free to subscribing schools and at a charge for non-subscribing schools.

If there are CPD events that you would like us to run then please let us know.

We are aware that at this time of year people may be changing role or moving school and taking on a new role. Please can you remind people to keep their CPD online details up to date so that your leaders receive the right targeted information and do not miss out on key opportunities. If you have new staff please contact the CPD team to get them added to your school establishment on ststraining@southglos.gov.uk

Contact details

For further information contact the team using the details below:

Jo Briscoombe

Role: Teaching and Learning Adviser ICT, CPD Lead, Online Safety and Online platform

Tel: 01454 863349

Email: jo.briscombe@southglos.gov.uk

Deb Ferris

Role: Teaching and Learning Adviser ICT and Maths, NQT Adviser, Online safety and online learning

Tel: 01454 868385

Email: deb.ferris@southglos.gov.uk

Website with link to our subscriber site
www.integra.co.uk