e-Safer Suffolk

Schools' choice

e-Safety
Parent & Carers
Awareness Training

Delegate Workbook

2014 – 2015

CONTENTS

Welcome to your e-Safety Awareness Training

Welcome

A warm welcome to your e-Safety Parent & Carers Awareness Training workbook; we trust that you will find it informative.

e-Safer Suffolk Team

Aim

The aim of today's session is for participants to be aware of what e-Safety is, to build their e-Safety skills and grow the confidence to deal effectively with an e-Safety incident or issue.

Objectives:

- To understand e-Safety in the context of illegal and/or unsuitable material.
- To be aware of children's online behaviour and consequences
- To know who to consult if concerned about a child at risk from their use of the internet.
- To be aware of the gaming age restrictions
- To be able to identify e-Safety issues including: -
    - 'Sexting' & sexual offences
    - Cyberbullying - malicious communications
    - Game ratings (PEGI)

What is the lower age limit to have a Facebook account?

A. 10

B. 12

C. 13

D. 16

Which of the following best describes Tinder?

A. A Dating App

B. Friendship Finder

C. A music download service

D. A location based area guide

Which of the following best describes ASK.fm?

A. A radio station

B. An anonymous social networking website where users can ask other users questions

C. A website which answers common questions on different topics

D. A podcast service

Which of the following best describes Snapchat?

A. A dating app where users are matched

B. A gaming app where users match up images

C. A messaging application for videos and images

D. A quick text messaging service for close friends

Which of the following is a fake social networking site or service?

A. Mateswappr?

B. Tinder

C. Chatroulette

D. Friendfinder

Who can your child send messages to on Chatroulette?

A. Only their Facebook friends

B. Those within their social network

C. Anyone with a webcam

D. Registered users over 18

According to a survey (Knowthenet), which site is being used most by 11 year olds?

A. Facebook

B. Instant Messaging

C. WhatsApp

D. AskFM

What proportion of children sign up to WhatsApp underage?

A. Less than 10%

B. 11% - 30%

C. 31% - 50%

D. Over 50%

Key Messages

Children, Young People & Vulnerable Adults

- Cyber bullying stops here!
- Sexting is illegal.
- If it happens, report it.
- If someone tells you about it, don't ignore it, do something about it.
- Suitability of games and apps must be taken seriously.

Key messages for Parents

- By creating e-Safer communities we aim to enable parents and carers to understand the risks.
- Parents must also be empowered to report concerns about what their children encounter online.
- You, as parents/carers, have a key role in providing safeguarding support for children.
- Be aware of what you are purchasing and how it will affect what your children do.
- Be aware of your online profile and how it can affect your children and the school they attend.
- Help to create an e-Safer Suffolk together.

Parents Can Read Slang

TXT	I Think It Means	It Actually Means
LOL		
88		
9		
99		
?^		
ADIDAS		
MIRL		
MIH		
RUS		
TTG		

The Strategy

Raising Awareness

AIM: That everyone including children and young people, their families, vulnerable adults and those who work with them are aware of the potential safeguarding issues and know where to go for advice, information and support.

Building e-Safety Skills

AIM: To ensure all children and young people and vulnerable adults in Suffolk remain safe and act responsibly whilst using developing technology including the internet and online gaming facilities.

Creating e-Safer Communities

AIM: To create e-Safer communities where e-Safety is embedded in everyone's policies, commissioning and planning activities, in order to prevent and appropriately respond to safeguarding matters.

Notes Page

PEGI Ratings

PEGI has 5 age categories

3: Suitable for ages 3 and older. May contain mild violence in an appropriate context for younger children, but no explicit language is allowed.

7: Suitable for ages 7 and older. May contain mild, cartoon violence, sports, or elements that can be frightening to younger children

12: Suitable for ages 12 and older. May contain violence in a fantasy setting, coarse language, mild sexual references or innuendo, or gambling

16: Suitable for ages 16 and older. May contain explicit violence, strong language, sexual references or content, gambling, or drug use (encouragement)

18: Suitable for ages 18 and older. May contain graphic violence, including "violence towards defenceless people" and "multiple, motiveless killing", strong language, strong sexual content, gambling, drug use (glamorisation), or discrimination

PEGI Content Descriptor

Icon	Content descriptor	Explanation	Corresponding age ratings
	Violence	May contain scenes of people getting injured or dying, often by use of weapons. Also may contain gore and bloodletting.	7 12 16 18
	Bad Language	May contain profanity, sexual innuendo, threats, and all manner of slurs and epithets.	12 16 18
	Fear / Horror	May contain scenes that are considered too disturbing or frightening to younger players.	7 12
	Sex	May contain references to sexual attraction or sexual intercourse. Also may contain nudity and characters dressed in suggestive clothing.	12 16 18
	Drugs	May contain references to illegal drugs or a fictional substance that has parallels to real-life illegal drugs (in use, possession, or sale).	16 18
	Gambling	May contain elements that encourage or teach gambling.	12 16 18
	Discrimination	May contain cruelty or harassment based on race, ethnicity, gender, or sexual preferences.	18
	Online	Contains an online game mode.	3 7 12 16 18

References and Further Reading

www.thinkyouknow.co.uk

- Practical advice and guidance for children, young people, parents and carers and professionals who work with children run by the Child Exploitation and Online Protection Centre (CEOP)

http://ceop.police.uk

- Go to this website to report concerns about a person's online sexual behaviour. (You can obtain the Click CEOP report abuse button for your web browser by contacting us at esafer@suffolk.gov.uk)

www.esafersuffolk.org

- Information and advice about e-Safety in Suffolk: Also gives an overview of the projects and activities of the e-Safety strategy which aim to make Suffolk an e-Safer place to be.

www.tso.co.uk

- Working Together to Safeguard Children 2010/2013: HMSO Sexual Offences Act 2003 www.legislation.gov.uk: HMSO.

www.pegi.info

- Provided by the Pan-European Game Information service, PEGI is a quick way to find the age ratings for computer games designed for Microsoft, Nintendo and Sony games consoles.

www.iwf.org.uk

- Use to report any harmful content including child sexual abuse images or incitement to racial hatred.

http://www.thesource.me.uk/

- The Source is Suffolk County Council's one-stop-shop for Children and Young People which includes a section on e-Safety with helpful videos and links to relevant websites and handy guides

Facebook Security Tips

1. Friends of friends = strangers. Be *really* careful about the "friends of friends" visibility option. It's a huge slippery slope that may invite a few thousand more prying eyes than you anticipate. As far as we're concerned, having this option is the same as going full-on public (which is fine, as long as you're fully aware of the risks of that level of visibility).

2. Preview your profile. Use the "view as" tab often. You can do this by clicking on the "gear" tab on your profile and scrolling down. You can see just how much you're revealing to the general Facebook public or to a specific person. With Facebook's ever-evolving privacy settings, you just never know what may have gone public by "default." Previewing your profile is one of the most decisive ways you can stay on top of this.

3. Choose your level of contact. You may not be able to hide from a search engine anymore, but you can control who can add you or message you (however, this function has become increasingly limited). With "basic" filtering, friends of friends/"people you may know" can message you, while "strict" filtering keeps it within the friends' circle. You can also choose to limit friend requests to "friends of friends" (you used to be able to opt out of requests altogether, but not anymore!).

4. Watch out for public photos. You may be tagged in any picture, but you can simply un-tag yourself. Use this power well.

5. Timeline approval is your friend. If you're a control freak, there's no way you don't already use this tool judiciously. But, if you're a bit more relaxed, you may still want to consider switching it on, so that all mentions and tags of you have to get your approval before appearing on your timeline at all.

6. Avoid accidentally landing your own ad campaign. You probably have third party apps linked to your Facebook without realising it, and this only further entrenches you in the grid. Some shady apps have come under fire for placing user images in their ads and have been banned from Facebook, but new ones can always spring up. Before installing any new applications, carefully read the fine print and think about what it's electing to do. You should also routinely manage your apps (under "main settings"), and delete where necessary. Somehow there's always one or two you either forgot about or, much like a virus, didn't know you invited into your digital life at all. You can also tell Facebook NOT to use your visage in any of its own ads by switching the "Facebook ads" option to "no one" under privacy settings.

Facebook Security Tips

7. **Keep your face on Facebook alone**. Turn off external search-engine visibility! (You can do this under "privacy" in main settings.) Facebook may not be the walled garden it once was, but you can still make it so no one without an account of their own can Google you.

8. **Use good judgment**. The ultimate precaution in staying secure online comes down to using common sense. You can always ask yourself:
"Would I want my boss/mother/colleagues/service users to see this?"
That goes for anything you do on any social media. Even with all your filters seemingly in check, if you really feel a pang of doubt, maybe err on the side of caution and simply live the moment without leaving a digital footprint. Not everyone needs to see all 11 eateries you checked into this weekend.

9. **For your eyes only**. There is an "only me" setting for just about every bit of profile data. This can work on anything from your relationship status, birth date, or education to a particular real-time update, etc.

10. **Deactivate!** Sure, like most things, it's scary the first time you do it, but then you realise it's not death — just a pause in your digital devotion might actually enhance your real life. To deactivate your account: Go to "settings," then "security" on the left-hand column, and then "deactivate your account." Breathe. Click. Done!

Twitter Security

Aiming to make it harder for outsiders to gain access to accounts, Twitter has now introduced a new, optional two-step login process, similar to that used by some UK online banking sites.

1. Register their mobile phone with Twitter. To do this, log in to Twitter.com and go to the cogwheel icon in the top right hand corner of your Twitter page, click on it and then 'settings'.

2. Scroll down to Account Security, where there's an option to 'Require a verification code when I sign in'. If you haven't registered a phone number, Twitter will offer you a link to do so, and the verification code option will be greyed-out until your phone is activated. Click the link to register your phone.

3. When prompted, text 'Go' to 86444 if you're in the UK.

4. Twitter will confirm that your mobile is activated.

5. Now click 'Require a verification code when I sign in', which should no longer be greyed out. If it is, you may need to refresh the web page.

6. Twitter will now send you another message confirming it can send verification codes to your device.

7. When you next log in to Twitter, a text message will be sent to your device, and you'll need to enter it to confirm your identity and complete the login process.

Note that you can currently only register one mobile per account.

Credit: Matt Warman, Consumer Technology Editor

Parents and Carers Checklist

I have asked my child to show me the sites they visit	
I have asked my child to set their profile settings to private	
I have asked my child about their online friends	
I have set appropriate parental controls on my child's computer	
I monitor my child's online activity	
My child has agreed to tell me if/when they're worried about something online	
I have access to my child's smartphone and tablet	
I have shown my child how to be e-Safer	
I know where to get help if I'm concerned about my child	

Think internet smart, internet savvy

Be internet savvy and make use of the security controls and privacy settings available on the technology, mobile devices and social networking systems that you and your child enjoy!

www.getsafeonline.org – how to protect yourself, your computer or mobile device and your business against fraud, identity theft, viruses and many other problems encountered online.

Enjoy the internet but be careful what sites your child visits. They can contain harmful content such as phishing malware that will try to access personal data for criminal purposes.

Adjust the security settings in their internet browser to make sure that they only visit 'safe' websites

Set up the security software on their pc, tablet or mobile to scan websites and apps before they open/download

Share only what you would not be embarrassed to share. Remember that your Facebook friends could also share pictures of you with others. So review your privacy settings on a regular basis.

NOTE: the LEGAL age for having a Facebook page in the UK is 13

Go to www.facebook.com/help/privacy for instructions on how to change your privacy settings

Vodafone Digital Parenting

How to set up the Vodafone Guardian app

The Vodafone Guardian app helps to keep children safer when using a smartphone.

As part of Vodafone's commitment to supporting parents in encouraging their children's safe and responsible use of digital technology, it offers the free Vodafone Guardian app for use on a range of Android devices.

Vodafone Guardian helps parents to manage their child's smartphone by providing protection from inappropriate calls, messages and online content.

The app enables parents to stay in control in a number of ways, including:

→ Blocking specific contacts or mobile phone numbers to prevent bullying text messages or calls

→ Specifying times during which their child can make or receive calls, use apps, access the Web and use the camera

→ Restricting outgoing calls to named contacts, such as Mum, Dad or specific friends

→ Transferring bullying text messages to a secure folder on the phone that could be used as evidence with the child's school or the police

Vodafone Guardian is available to download for free from Google ™ Play.

Step 1

- **Set a Parent Contact**

Once you have downloaded the app, enter a parent contact number so that you receive a text whenever Vodafone Guardian is deactivated for any reason. Click 'Save'.

You will also receive a text when an emergency call is made from the handset. Calls to ChildLine numbers are always allowed, you are not notified, and Vodafone Guardian removes the log entries for such calls.

Step 2

- **Choose a password**

You can set a password so that you control the app. No changes can be made to the Vodafone Guardian settings without this password.

Simply enter your password twice and click 'Save'.

Step 3

- **Enable Message Helper**

If you enable Message Helper, Vodafone Guardian will show an 'I Do Not Accept This' button next to incoming messages. Pressing that button will make the message vanish from your child's in-box and it's there to help them if they get an unwanted message.

Go to Message Helper and choose 'always enabled', 'never enabled' or 'Enabled between' (and enter your chosen hours and days).

Step 4

- **Customise the settings**

You can customise the settings for calls, text messages and phone features, such as Wi-Fi, Bluetooth, Camera, Browser and Adding and Removing Apps. For example:

→ If you want to set a time schedule for when your child can receive or make calls or receive texts, click on 'Calls & Messages' then 'Active Hours' and choose the time limits. This is useful for limiting how your child uses their mobile during school hours or after bedtime, for example

→ If you decide that you'd prefer your son or daughter to not have access to the internet at all from their mobile, go to 'Phone Features' then 'Browser' and choose 'Never allowed'

→ To prevent use of the camera while they're at school, go to 'Phone Features' then 'Camera' and set the timer underneath 'Allowed between'

Vodafone Guardian has been developed by the Vodafone Foundation (registered charity no. 1089625) as part of its Mobile for Good programme.

Key Contacts

Nathan Simmonds

SLQA Training Manager e-Safety

Fran Southwell

SLQA e-Safety Peer Ambassador

Jana Bednarova

Business Support e-Safety

esafer@suffolk.gov.uk

www.esafersuffolk.org

Course Evaluation

Name: (Please Print)	
School/Organisation:	
Your Job Role:	
Contact Telephone No.	
Date:	
Facilitator:	
Course Title:	Suffolk e-Safety Parent & Carers Awareness Training

How would you rate:	**Poor 1**	**Fair 2**	**Satisfactory 3**	**Good 4**	**Excellent 5**
Your overall learning experience					
The trainers' knowledge of the subject					
Did the delivery style meet your learning need?					
Did the content meet your expectations?					

What did you find most useful?	
What could have been done better?	
What will you now do to safeguard Children, Young People & vulnerable groups as well as yourself as a result of this training?	
Any other relevant comments.	

Created September 2014
Version 2.0
Safeguarding Learning & Quality Assurance
Publication Ref- **014-P&C-230914**