Online Safety Newsletter

Spring 2019

Issue 3

Contents

Welcome

Welcome to the third edition of the Online Safety Newsletter produced by members of the E-Safety Working Group. It has been a busy time for the team with our second online safety conference taking place in January. This event entitled 'Putting online safety in context' highlighted the importance of **'Contextual Safeguarding'** which is an approach to understanding and responding to, young people's experiences of significant harm beyond their families. This was a fantastic event attended by over 200 delegates from educational settings as well as

multi- agency partners. Key note speakers included: Alan Earl Former Harm Reduction Officer SWGfL and Police Officer Avon and Somerset Police; Lorin LaFave - founder of 'The Breck Foundation' and representatives from the BSCB Shadow Board. In the afternoon delegates attended a number of workshops covering a range of online safety issues including: cyberbullying, sexting, parental engagement and school staff and their use of social media. Resources from the conference are available here.

Please help to spread the word about this newsletter and encourage colleagues to access it via the BSCB website.

BSCB E Safety Working Group

News

Instagram biggest for child grooming online- NSPCC finds

Sex offenders are grooming children on Instagram more than on any other online platform, a charity has found. According to the NSPCC, Police in England and Wales recorded 1,944 incidents of sexual communication with children in the six months to September 2018. Instagram was used in 32% of the 1,317 cases where a method was recorded, Facebook in 23% and Snapchat in 14%. The full article can be found on the BBC website.

Momo Challenge

Earlier this year schools and parents were alerted to concerns about the Momo ‘Challenge’. The exact nature of the ‘challenge’ is hard to define and more details of this internet phenomenon can be found in articles by the Independent and Net Family News.

Joanne Bocko, Cyber Protect Officer from Avon and Somerset makes the following comments regarding this and other viral ‘challenges’ -

She said, “the tricky part is managing the fear felt by parents whilst not over–promoting the ‘game’, therefore bringing it to the attention of our young people who, for the most part, are oblivious to these viral games and challenges. Our advice for parent/carers is not to focus on any specific challenges or trends, but instead to:

- Ensure you know what your children can access online;
- Make sure children understand the importance of not giving personal information to anyone they don’t know;
- Tell your child no-one has the right to make them do anything they don’t want to do;
- Use parental controls to keep children safe;
- Explain you should not talk to anyone you don’t know online;
- Keep the lines of communication open and keep talking to your children about online safety.

Further advice is available from the BBC for children if they see something scary online and what they can do.

Starter Packs

Starter packs (or starter kits) are a collage of photos, GIFs, text clips, screenshots, colors, and quotes that perfectly illustrate a particular identity, experience, subculture, or abstract concept. Starter Packs are great for bringing a community together since everyone can relate to the elements in it. A Starter Pack not might make sense to anyone else, but, to members of that subculture, it's hilarious and nostalgic. The more specific, the better! However, the problem arises as people are able to create their own "starter packs" that are used to insult, mock and bully others. Whilst many starter packs can be harmless fun, school staff and parents need to be aware of the potential for starter packs to be used as a tool to cause harm and distress.

SWIGGLE

Building effective online search skills in children and young people is vital in ensuring learners get to the information they need for their studies. After 18 months of development, the Online Safety experts at SWGfL are proud to announce the launch of a new child friendly search engine, Swiggle.org.uk. For more information about this product specifically aimed at KS2 pupils please click here.

Apple Screen Time

Screen Time — a new feature of iOS 12 — lets you know how much time you and your children spend on apps, websites, and more. This way, you can make more informed decisions about how you use your devices, and set limits if you would like to. For more information visit the Apple website.

Filtering - Update

In During the February half-term, the Trading with Schools ICT Team migrated to a new internet filtering system called Netsweeper. Information about this was given in the last issue of the Newsletter too.

Netsweeper is very powerful and gives schools access to lots of information. As a minimum, we recommend that Designated Safeguarding Leads (DSLs) ensure they are receiving regular reports regarding information about Prevent. Please contact the ICT Helpdesk to set this up by emailing schools.it.helpdesk@bristol.gov.uk.

Customisable reports can also be set up, where the system will alert you if a certain word has been searched for or a certain website accessed. This is useful if you are facing a particular issue in your school.

Schools are able to customise their own block pages too. This is useful particularly if websites fall into categories such as self-harm where you may want to signpost to resources where help can be sought.

If you are a DSL for more than one school or for a MAT, you can also access information for all the schools you work across.

One thing that is vital for the system to work properly is for all your users, both staff and students, to have their own unique usernames. If you do not currently have this facility set up, we recommend contacting your ICT Support Provider as a matter of urgency.

Everything described above can be set up by contacting the ICT Helpdesk. The helpdesk staff are keen to get the provision right for

schools and are more than happy to answer questions and set things up for you. Please do get in touch with them. Their email address again is schools.it.helpdesk@bristol.gov.uk.

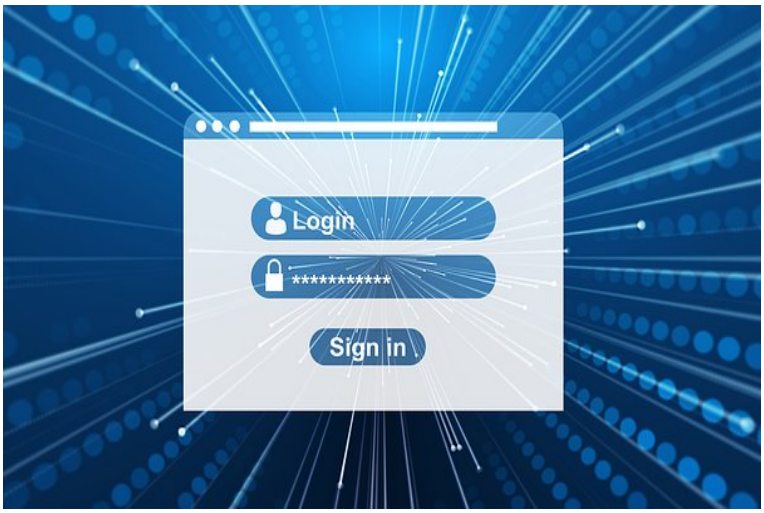
Latest Games and Apps

Discord

Discord is an app utilised by gamers to speak with each other whilst playing live online games. Users can add friends, local players or join in wider group chats. Users can login with a username, and they can add friends, join a server, chat by logging in with a code provided from an email invitation or from a real-life friend. Users can send direct messages to other users, chat, and talk or listen in larger group chats. Using the Nearby feature when adding friends (and with location features turned on), you can find users near you. For a full review of the app please visit Commonsense Media.

Sharing Practice

Password Security



With young people signing up to online apps and accessing different systems both at home and school, it is important to equip them with information about how to create strong and secure passwords.

Recent research from Splashdata evaluates over 5 million leaked passwords used on the internet and looks at the most common ones used. Perhaps unsurprisingly, the top 2 remained unchanged in 2018 with 123456 at number 1 and password at number 2. At number 3 is 123456789 and number 4 is 12345678, an interesting new addition is this one - !@#$%^& - which looks pretty strong at first glance, until you realise that it's basically 1234567 whilst holding the shift key.

Trying to remember passwords for all the different programs you access can be challenging, but it is worth putting some effect into getting it right, so access remains as secure as possible.

Some tips you can use when advising young people;

- The longer a password is, the harder it is to crack
- If there is complexity in it, it becomes more secure e.g. changing a letter for a number or inserting punctuation so exchange E for 3, or I for ! – the word levels could become L3ve!s

- Pick something personal but easy to remember (not a birthdate or address) maybe a favourite song title or make and model of a car
- Use a minimum of eight characters for your password, preferably upwards of 12 characters
- To help remember passwords right a tip sheet as a prompt.

And give advice about how to keep access secure on an ongoing basis;

- Try to avoid password reuse across multiple sites
- Ensure that when you finish on a device you log out completely so people can't access your accounts and information.
- Don't share you passwords with friends
- Think about changing passwords regularly and avoid reuse within a year.

Secure access to their information can protect them from fraud, identity theft and misuse of their accounts for malicious purposes, it's all part of making them aware of how to keep themselves safe online.

Help and Support

Early Years Online Safety Advice

Following on from feedback from the 2018 BSCB Online Safety Conference, we were aware that online safety resources for providers

of care and education within the Early Years Sector were a little lacking.

So, in an attempt to address this, the members of the E Safety Working Group pulled together a range of information, resources and guides for both practitioners and parent/carers to support the early intervention and support needed for young children to help them build resilience and understanding in how to begin to keep themselves safe online.

The resources that were pulled together are available from the BSCB Website.

Also, since the conference, CEOP (Child Exploitation and Online Protection) via their support website Thinkuknow have released a range of support resources based on Jessie and Friends. This is a 3 episode animated series which aims to equip 4-7 yr olds with the knowledge, skills and confidence they need to help them stay safe from sexual abuse and other risks they may encounter online. They can be downloaded from here, along with a professional's resource pack and advice for parents.

Feature Website

The Breck Foundation is a charity founded by Lorin LaFave after the tragic loss of her 14 year old son Breck Bednar through internet grooming.

Using Breck's story, Breck Foundation Speakers travel the UK educating the Digital Generation to keep safer online. They campaign for a safer internet and help train police, educators, health practitioners, safeguarding leads, parents and pupils to ensure that young people are empowered to make safer choices for themselves online.

The Foundation provides links via their website to resources for parents, carers and teachers including the video 'Breck's Last Game'.

Pass it on

Avoiding the Scams

Scams take many forms but there are some common ones to look out for including bank scams, phishing, pharming and sextortion.

Bank Scams

Someone may call you and claim to be from your bank. They may inform you that there is a problem with your account and ask for information. Remember your bank will never ask you for your card PIN nor will they suggest you transfer money to a 'safe account'. If in doubt hang up and call your bank to verify the problem.

Phishing emails/texts

This is when an email or message is used to trick you into providing personal information. You might receive a text or email claiming to be from your bank or other trusted provider like HMRC or your local council. Make sure you check the sender's email address, it should match the official website of the provider e.g. info@hmrc.info will not be from hmrc.gov.uk.

'Pharming'

A common trick used by scammers to redirect traffic from a legitimate website to a fake version where they can collect information. This is different from phishing because you are likely to be trying to access a real website, watch out for this tricky attempt. Often these websites will model the original but look low budget and may not have many pages. e.g. hmrc.gov.uk will never be hmrc.co.uk.

Romance Scams/Sextortion

This is when victims are groomed into false relationships by someone who aims to gain their trust, eventually stealing their money or accessing their personal information. A quick reverse image search of their profile picture will show you where else it has been used. Be aware of 'things moving too fast' and remember that personal or sensitive things you say

or share (including images) could be used against you. If this happens, the emotional impact can be overwhelming. It's illegal to blackmail people online, If this happens to you, you should contact the police immediately who will be able to help.

The first step in being 'scam aware' is to support children and young people to understand the **different ways** that someone might be trying to scam them. Scams can evolve quickly use adapting techniques, but luckily there are a few consistent themes in fraudulent scams that you should advise children and young people to look out for:

- Generally speaking, if it sounds too good to be true - it probably is.
- Scenarios or alarming claims, news or threats that make you feel pressurised into acting.
- Being asked for personal information or bank details - there is usually money involved.

FFA UK and Telecommunications UK Fraud Forum (TUFF) run an initiative to teach young people (aged 7 to 16) about:

- the responsible way to operate and safeguard a mobile phone
- the value of personal information and how to protect it
- the importance of online security and how to avoid becoming a victim of fraud.

Out of Your Hands is a schools' resource aligned to the National Curriculum featuring example scenarios of typical fraud scams, mobile phone crime and guidance on how to stay safe when making online transactions as well as real-life victim and perpetrator case studies and

short films. The resources raise awareness of scams such as Vishing, Money Muling and courier fraud, as well as helping young people consider the risks of sharing their personal information with others.

The Out of Your Hands initiative has three distinct strands as follows:

Out of Your Hands aims to educate young people about the impact of mobile phone crime and teaches responsible mobile use.

Out of Your Pocket aims to educate young people on how to avoid becoming a victim of fraud. There's information about typical scams, what to look out for in suspicious emails, and how to stay safe when making decisions and transactions online.

Out of Your Control aims to stop young people from becoming victims of identity theft and online crime by teaching them methods to protect their private data and to be confident when they are online.

Visit www.outofyourhands.com to find out more and sign up for regular information.

In acknowledgement that some people are more vulnerable to scams and fraud, Action Fraud offer enhanced services including additional support, counselling and information for vulnerable victims, such as:

- Anyone under the age of 17.
- Anyone living with a mental health issue within the remit of the Mental Health Act 1983.
- Anyone with a SEND needs.

To access this support for young people you are working with you can use their online reporting tool, or by calling them on 0300 123 2040 making it clear you are reporting on behalf of a vulnerable person so that they receive the right support.

Contextual Safeguarding

Internet Safety 14+

The Thinkuknow website has toolkits for all ages, with resources and lesson plans to support children and young people in understanding online safety and the risks they might encounter.

Thinkuknow have recently updated the toolkit for those aged 14+ so they can learn more about sharing nude images, what the law says and how to protect themselves and others.

Alongside this, the website tackles a wide range of issues including child sexual exploitation, pornography and digital dating. Supporting young people to explore the information on Thinkuknow.co.uk will help them to:

- Develop healthy approaches towards sex and the Internet
- Identify and respond to negative behaviour online

Events

Ever thought of becoming a CEOP Ambassador?

The Child Exploitation and Online Protection (CEOP) Command, under the National Crime Agency, offers courses for professionals to become CEOP ambassadors.

The CEOP Ambassador course provides an in-depth look at:

- Introduction to CEOP and reporting
- How children and young people use the internet, social media and online technologies
- The nature of online sexual offending against children and young people
- Dealing with incidents of youth produced sexual imagery
- How to deliver strong preventative education on online sexual abuse and exploitation across age groups

If this is of interest to you, you can find your local course here.

For further information and any questions in relation to this newsletter please contact the Bristol Safeguarding Children Board at: bscb@bristol.gov.uk