The Digital Generation

freedom from abuse

V 18.06

Contents

'The Digital Generation' is brought to you by

freedom from abuse

Connected Minds

Foreword

Marilyn Hawes
Founder and CEO
Freedom from Abuse C.I.C.

Love it or hate it, beauty AND beast; the Internet and apps are here to stay and social media is very much an organic living part of our lives. NOBODY, least of all us , are saying STAY AWAY! That would be ridiculous.

Over the last decade I have drawn together information about the Internet when it became obvious how rapidly it would grow and become a strident teenager! However the Internet now, has grown beyond my initial expectations.

I decided this ORIGINALLY short document was required and would be perfect for parents to stay up to speed with what is what. I then named it the DIGITAL GENERATION as clearly today's youngsters are JUST that! As time progressed, I was updating it every week to stay abreast of all the information.

It was remarkable when a few months ago I was contacted by Gareth Cort who had seen the document at a school where he was presenting at the time. He offered to help work with me and produce this new document which is beyond recognition from the format. I am hugely proud of what has been achieved.

We will be regularly updating the information on the News section as various apps come long, and what to avoid and essentially how to stay safe.

There are so many benefits to life online, but it is not without its risks. **Education** is key to empowering children to manage online risk and make the most of their time online or with technology.

It is easy to think of the current generations (Generations Z and Alpha) as being 'digital natives' as the technology and services in everyday life have been around for most or all of their lives. However, having always lived in a world of social media, smartphones and online gaming doesn't mean that they instinctively possess the skills or knowledge to keep themselves or others safe. Therefore, providing opportunities to discuss online experiences with children and young people is crucial. It enables them to recognise the potential risks, develop strategies to handle them positively and know how to give and receive support.

Keeping up to date with the latest trends, advice and resources in this area is no easy task, so we have developed 'The Digital Generation' as a quick way to get up to speed on issues and advice relevant to the children you work with.

The sections of this document can be separated and read independently of each other so please do share this document with colleagues in your school and further afield and do get in touch if you have any questions or require further support.

Gareth Cort
Online Safety Specialist
Connected Minds Ltd.

If you have any questions or comments about 'The Digital Generation' then please do not hesitate to contact Gareth at **gareth.cort@ff-a.uk** or Marilyn at **marilyn.hawes@ff-a.uk**.

What's in the news?

It can be a huge challenge to keep up to date with the latest games or apps that children and young people like to use, as well as the daily media coverage of issues and developments related to the internet.

This section aims to provide a quick update of the latest stories and events that relate to the lives of young people. These can provide an excellent starting point for discussions around how to use the internet positively and safely. Take time to listen to what young people have to say about these stories; it can provide you with great insight as to how they perceive risk, what choices they might make when faced with a problem and may give you enough information to take further action. It is not uncommon for disclosures to be made when discussing online activities; always ensure that you follow your school's safeguarding procedures to record these and inform your Designated Safeguarding Lead (DSL).

Last updated: June 2018

June 2018

Don't be afraid to take phones off teens, says Eton head

Schools and parents should not be scared to take away smartphones and other devices off teenagers. It removes the pressure of having to check the device at night time says headmaster of Eton. **Don't be afraid to take phones off teens, says Eton head (BBC News, 13th June 2018)**

Stand Up to Bullying Day (13th June 2018)

Started in 2016 with support of HRH The Duke of Cambridge, the day encourages young people to be upstanders rather than bystanders. Free campaign packs and materials are available on the site. **standuptobullying.co.uk**

Fortnite Battle Royale grows to 125 million players in less than a year

Popular online game Fortnite has gown to 125 million players. Between 2018-2019, the publisher Epic Games will be running competitions with a $100 million prize pool. **Announcing 2018-2019 Fortnite Competitive Season (Epic Games, 12th June 2018)**

Online comments putting 'unfair pressure' on teachers

A Welsh teaching union suggests staff face 'trial by social media' from parents making accusations and threats online. A social media expert argues that schools need to connect more with parents online. **Online comments putting 'unfair pressure' on teachers (BBC News Wales, 1st June 2018)**

May 2018

Police to treat gangs like terror suspects with tough new laws

Police and CPS are considering using legislation to treat gang members as terrorism suspects if they are using 'drill music' videos on YouTube and other social media to incite violence. **Police to treat gangs like terror suspects with tough new laws (The Telegraph, 30th May 2018)**

New data protection legislation comes into force

The General Data Protection Regulation (GDP) came into effect on 25th May 2018. It give people more control over the use and storage of their data, as well as imposing age restrictions on social media. **New data protection laws put people first (ICO, 25th May 2018)**

More than half of 12 year olds have live-streamed content, survey says

Barnardo's found that 57% of 12 year olds and 28% of 10 year olds had livestreamed. Almost 1 in 4 of those aged 10-16 said that they or a friend had regretted posting something live. **More than half of 12 year olds have live-streamed content, survey says (Barnado's, 24th May 2018)**

What's in the news?

May 2018 cont.

UK Government publishes response to the Internet Safety Strategy Green Paper

Aiming to make Britain the safest place in the world to be online, the strategy considers the responsibilities of companies to their uses, technical solutions to prevent online harm and the government's role in supporting users. **Government response (HM Government, 20th May 2018)**

Updated Keeping Children Safe in Education statutory guidance published

Live from 3rd September 2018, the DfE's updated guidance includes a greater importance on training for DSLs, vulnerabilities of SEN pupils, sexual violence and harassment between pupils, and child exploitation (criminal and sexual). **Keeping children safe in education (DfE, 17th May 2018)**

Research on child sex abuse live-streaming reveals 98% of victims are 13 or under

A study by the Internet Watch Foundation of child sexual abuse images captured from livestreamed video found 98% of victims were aged 13 or younger and 28% were aged 10 or younger. **IWF research on child sex abuse live-streaming reveals 98% of victims are 13 or under (IWF, 12th May 2018)**

1 in 4 young people have been contacted over social media by an adult they don't know

The NSPPC and O2's survey of children and parents also found Twitter and Reddit ranked highly for inappropriate content and Facebook and YouTube ranked high risk for violence, bullying and adult content. **1 in 4 young people contacted online by an adult they don't know (NSPCC, 2nd May 2018)**

April 2018

Google introduces new choices for parents to further customize YouTube Kids

Three new parental control options were introduced for the YouTube Kids app - collections/channels by trusted partners, parents to approve content and better 'search-off' functionality.
Introducing new choices for parents to further customize YouTube Kids (YouTube, 25th April 2018)

WhatsApp raises minimum age to 16 in Europe

Ahead of the introduction of the GDPR across the EU in May 2018, WhatsApp has amended its terms of service to raise the minimum age of use from 13 to 16. Users will be prompted to accept a new terms of service and updated privacy policy. **WhatsApp raises minimum age to 16 in Europe ahead of GDPR (The Guardian, 25th April 2018)**

IWF 2017 Annual Report published

The Internet Watch Foundation publishes its 2017 Annual Report with the latest data on what's happening globally to tackle child sexual abuse images and videos online.
IWF 2017 Annual Report (IWF, 18th April 2018)

Facebook tops list of sites used for online grooming

Figures from the NSPCC's Wild West Web campaign found 32.6% of grooming cases involved Facebook use and 18.8% of cases involved Facebook owned apps Instagram and WhatsApp.
Facebook tops list of sites used for online grooming (NSPCC, 16th April 2018)

Safer Internet Day 2018 reaches 45% of young people in the UK

The Safer Internet Day 2018 Impact Report found 45% of young people aged 8-17 and 30% of parents heard about SID2018. 1,772 organisations supported the day and over 9.1 million people were reached via social media. **Safer Internet Day 2018 reaches 45% of young people in the UK (UK Safer Internet Centre, 10th April 2018)**

Online grooming

Definition

Online grooming is when an adult contacts a child online to build a relationship or emotional connection to gain trust in order to **abuse**, **exploit**, **radicalise** or otherwise **harm** them. This harm may take place purely online or may be part of a process in which an adult intends to

How does it happen?

Grooming can take a number of different forms online and can occur on **any game/app/social media service** that is frequented by children or young people.

Some instances of online grooming involve a stranger disguising their true identity and intentions; they may strike up a friendship with a young person in an online game or social network by pretending to be the same age and either the same or opposite gender (e.g. pretending to be a 14 year old girl to attract teenage boys). This is often known as **'catfishing'**.

However, an abuser's methods depend on their preferences. Research from the University of Swansea and NSPCC Wales found that most of the approaches by adults involved no deception around them being an adult. In 75% of cases studied the target was **female**. Commonly, targets were aged **12-15 years old** and the grooming incurred frequently on **social media**.

The research also identified three distinct phases of grooming; **access, entrapment and approach**. Analysis of over 140,000 words from online chat logs also suggested that groomers were sophisticated communicators who used persuasion rather than coercion to build trust.

Methods to achieve this include:

- **Researching** about the young person online; finding out as much **personal information** as possible so a groomer knows who that young person is, what their likes/interests are, who their friends/family are, etc.
- **Complimenting** a young person on a range of topics (not just sexual themes), attempting to make them feel special.
- **Isolating** a young person from their friends, family and community by suggesting that those groups don't understand or care about that young person.
- **Testing boundaries** and willingness to comply with a groomer's requests; most groomers contact multiple young people so that they can quickly move on to another target if it appears that a young person is unwilling to do as they wish. In cases of grooming for sexual purposes, this also ensures that the sexual gratification a paedophile gets from having such contact with children goes uninterrupted.

Sexual exploitation and abuse online

Children who are persuaded or forced into harmful behaviour may engage in:

- Sexual messages/conversations.
- Creating and sharing sexual images/videos of themselves.
- Performing sexual acts via video chat on a webcam or device with a camera (e.g. smartphone/tablet).
- Meeting up offline with the groomer and being abused physically.

Online grooming

Signs that a young person is being groomed online

Some of the following behaviours may indicate that a child is being groomed:

- Become more secretive about all aspects of their life, including how they use the internet.
- Display changes in mood or personality.
- Display signs of inappropriate sexual behaviour for their age.
- Become withdrawn/isolated from those around them (friends and family).
- Show other sudden behaviour changes including the use of drugs or alcohol, greater risk taking or self-harm.

Advice for staff

- Be alert - look out for any behaviour changes in the children you work with.
- Follow safeguarding procedures - repot any concerns to your Designated Safeguarding Lead (DSL) and record your observations/conversations with a child that have led to your concerns.
- As of April 2017 it is now illegal for an adult to send a sexual message to a child under the Serious Crimes Act (2015).
- If you have concerns or suspicions that a child is being groomed online then report this to the National Crime Agency's CEOP Command at ceop.police.uk. Ensure your DSL is aware so that they can support you and access further help as required.
- Educate the children you work with on the risks of online communication with strangers, the strategies they can use to look after themselves and others, and how to get help if they are worried. Promoting the importance of looking out for others online is imperative; someone being groomed may not recognise it, but others around them could.

Resources for schools

- **Play, Like, Share** - CEOP's resources aimed at primary age for teaching and discussing sexual exploitation online.
- **Exploited** - CEOP's film for ages 14+ about online relationships and the risk of sexual exploitation and abuse.
- **The BLAST project** - Resources by Yorkshire MESMAC for educators to use to encourage reporting and recognition of grooming risks.
- **The Life and Death of Breck Bednar** - Resources by BBC Three on the tragic story of Breck Bednar.

Resources for young people

- **Think U Know** - CEOP's site has sections containing information and advice for different age groups.
- **Childline** - Childline's site has information about online grooming and advice for young people if they are worried.
- **Kayleigh's Love Story** - A hard hitting film for age 13+ by Leicestershire Police of a real life grooming case that ended in tragedy.

Further reading

- **Barnardo's' survey on online grooming** - A snapshot survey of five Barnardo's sexual exploitation services showing the prevalence of online grooming and sexual exploitation.
  Fox & Kalkan., 2016

Child abuse content

Definition

Child sexual abuse content are images that create a visual record of the sexual abuse of a child. This can include **images, photographs, pseudo-photographs, animations, drawing, tracings, images and videos.** These forms are sometimes referred to as 'indecent images of children' (IIOC); particularly when discussing content created by sexting behaviour between young people.

How is this content categorised?

Under the Sentencing Council's Sexual Offences Definitive Guidelines, child sexual abuse content can fall into one of three categories:

A	B	C
Images involving penetrative sexual activity and/or images involving sexual activity with an animal or sadism.	Images involving non-penetrative sexual activity	Other indecent images not falling within categories A or B

The Law

In the UK it is illegal to create, possess or distribute child abuse content under the following laws:

- **Protection of Children Act 1978 -** England and Wales
- **Civic Government (Scotland) Act 1982 -** Scotland
- **Protection of Children (Northern Ireland) Order 1978 -** Northern Ireland

Why is it harmful to children?

These images and videos can be shared and viewed repeatedly across many sites and services and across time. For a child who appears in this content, this feels like being abused over and over again. While efforts are made to remove this content online, there can **never be a 100% guarantee** that the content is truly 'gone', which can worry and affect victims throughout their lifetime.

Access to this content also encourages abusers to commit similar acts and fuels the needs of paedophiles to view such content. Worryingly, the IWF's annual report in 2016 saw a large increase in 'self-generated images' (images/videos that children have taken of themselves via webcam) amongst reported child abuse content. Therefore, educating children about the risks of taking and sharing these sorts of images is key to prevent avoidable abuse.

Where is it found online?

This content is most commonly found on **image hosting sites** and **cyberlockers** (cloud storage). Access to such material may require specific files (such as cookies) present on a device to 'unlock' hidden images on a site. Peer to peer file sharing services are also a popular choice as they can be encrypted to prevent access from the service provider or law enforcement. Increasingly, criminals are using 'disguised websites' to hide child abuse content and leave clues for other paedophiles on how to find it. THE IWF saw an 86% increase in the number of disguised websites reported to them. *(Source: IWF Annual Report 2017- IWF)*

Child abuse content

Where is it hosted?

0.3%

Of child sexual abuse content is hosted in the UK

The top five hosting countries:	Percentage of reports (2017)
Netherlands	36%
United States	18%
Canada	15%
France	10%
Russia	8%

Source: IWF Annual Report 2017 - IWF (2018)

Livestreaming

From a sample of 2,082 images and videos of livestreamed child sexual abuse, the IWF found:

98%

were of children aged 13 or younger.

96%

of the victims were girls.

100%

had been harvested from their original upload locations.

Source: Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse - *IWF (2018)*

Reporting

IWF Internet Watch Foundation

While it is rare to stumble across child sexual abuse content when browsing the internet in the UK, it is still possible to see such material.

If you do see content of this nature, you can report it to the Internet Watch Foundation (IWF), the UK hotline for reporting child sexual abuse content, at www.iwf.org.uk.

Further reading

- **IWF Annual Report 2017** - Provides statistics and information about the reports received by the IWF of child sexual abuse content online.
- **INHOPE** - Information on the International Association of Internet Hotlines, of which the IWF is a member.
- **Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse** - Research conducted by the IWF into the nature of abuse present in still images captured from livestreamed content. *IWF, 2018.*

Sexting

Definition

Sexting is when someone takes and sends naked, semi-naked or sexual images or videos, either of themselves or others. The term can also be used to describe sexual messaging but is most commonly used to refer to images and videos.

This can occur on any technology that allows messaging and sharing of content, such as phones, tablets, laptops/computers and other connected devices that possess a camera.

Risks

There are a number of risks associated with this behaviour that can negatively affect a young person's mental health and wellbeing, reputation and relationships. It is also behaviour that can break the law:

The Law

Under the **Protection of Children Act 1978** (England and Wales) it is illegal to create, distribute or possess an indecent image/video of someone under the age of 18. Therefore, a young person who has taken and shared a nude selfie would have broken the law, even if the photo was shared with other young people of the same age. It is also an offence to keep that image on their own phone, even though it is an image of them.

Law enforcement in the UK has always taken a balanced approach to young people sexting, with the National Police Chiefs Council taking the stance that these incidents should primarily be treated as safeguarding issues and that a criminal justice response would only be considered proportionate in certain circumstances. The College of Policing has issued a **briefing note to all forces in England and Wales** highlighting the need for a common-sense approach when investigating sexting incidents involving young people under the age of 18.

Outcome 21

As sexting incidents involving young people constitutes a 'crime', it must be recorded if reported to the Police, under Home Office reporting rules. All reported crimes also require an outcome code. From January 2016 onwards, police forces can apply Outcome Code 21 which states:

'Further investigation, resulting from the crime report, which could provide evidence sufficient to support formal action being taken against the suspect is not in the public interest. This is a police decision.'

However, the use of this code depends on the circumstances of the incident and may not be applied if there are other factors that necessitate a more formal response/sanctions e.g. a young person sharing nude images of another young person without consent as a form of harassment and bullying.

Other consequences to young people:

- Damage to relationships and friendships—a breach of trust and respect.
- Wider sharing of an image can lead to gossip and rumours that can damage a young person's self-esteem and wellbeing.
- Images/videos found online can negatively affect a young person's reputation.
- Shared images/videos can be used to bullying, to damage someone's reputation or to blackmail (often known as sextortion).

Sexting

Managing incidents

There are many ways that a sexting incident could occur in your school/setting and the nature of an incident is dependent on a number of factors such as the age of the children/young people involved, the nature of the content shared, how/where/why it was shared and the perceived impact on the young people involved.

Effective handling of any incident relies on treating it as a safeguarding issue and to follow your setting's existing safeguarding practice with regards to reporting, logging and escalating an incident. The safety and wellbeing of the young people involved should be central to the actions taken and any resulting investigation.

UKCCIS (the UK Council for Child Internet Safety) have produced **guidance for schools and colleges** on what to consider when responding to an incident, how to integrate actions into existing safeguarding structures and where to seek further help/guidance.

Advice for staff

- Don't panic!
- **Report any sexting incident involving young people to your Designated Safety Leader (DSL) immediately.**
- Follow your safeguarding procedures.
- (If possible) Confiscate the device containing sexting content and hand over to the DSL.
- **Do not** attempt to delete, copy, backup or share on the content.
- Provide support and reassurance to the young people involved.
- Look for educational opportunities e.g. running lessons and discussions around sexting, peer pressure, consent and relationships.
- Further advice is available from the **Professional Online Safety Helpline** run by the UK Safer Internet Centre on **0344 381 4772** or **helpline@saferinternet.org.uk**.

Resources for schools

- **Crossing the Line** - Childnet's PSHE Toolkit contains a film, lesson plan and activities on sexting.
- **Exposed** - A film by CEOP that explores how sexting happens in teenage relationships and the possible consequences.
- **Lockers** - A resource by Webwise covering many aspects of sexting. (Please note this was created for schools in Ireland and so references Irish law.)

Resources for young people

- **Content Reporting** - Childline have partnered with the IWF to offer a reporting portal for young people to report their sexting images online to be removed.
- **ZIPIT** - A free app by Childline to help young people resist peer pressure to take and send nude images/videos.
- **So you got naked online...?** - A guide by the SWGfL for young people on what to do if they are worried about sexting.

Further reading

- **"I wasn't sure it was normal to watch it"** - A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people. *Martellozzo et al., 2017*
- **The Conversation**—Articles detailing the latest news and research around sexting.

Sexual violence and harassment

Online sexual harassment

This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. In many cases, behaviour has both online and offline elements.

It may include:
- non-consensual sharing of sexual images and videos
- sexualised online bullying;
- unwanted sexual comments and messages, including, on social media; and
- sexual exploitation; coercion and threats.

Source: Sexual violence and sexual harassment between children in schools and colleges - DfE (2017)

Further explanation and examples of this behaviour and its effects can be found on **Childnet's Project deSHAME** page.

Young people's experiences

Childnet's Project deSHAME focuses on providing practical advice, guidance and teaching materials around online sexual harassment and violence, with an aim to increase reporting of these incidents.

The resources for young people, schools and police are due out in Autumn 2018.

Part of the project involved research of the experiences of young people in the UK, Hungary and Denmark; some of the key findings are below:

'Bait out' pages

These are pages (or groups/channels on social media) created by young people for others in their school or local area to share sexual gossip, sexual images and make sexual comments about individuals. This can include sexting images that have been shared on or photos/videos taken covertly of an unaware victim. It may also include 'naming and shaming' individuals and detailing their sexual exploits.

68% of respondents agree that people will think badly about a girl if her nude/nearly nude image is posted online. 40% would think the same for a boy.

80% had witnessed peers using words like 'sket' or 'slut' online to describe girls. 68% had witnessed homophobic or transphobic language.

52% wouldn't report online sexual harassment because they felt 'too embarrassed'.

50% wouldn't tell a teacher for fear that the school would overreact, 53% wouldn't tell the police because they didn't want their family involved, and 43% didn't think it would help to report it on social media.

Further reading

- **Young people's experiences of online sexual harassment** - A cross-country report from Project deSHAME. *Childnet et al., 2017*
- **Sexual violence and sexual harassment between children in schools and colleges** — Guidance from the DfE that links to Keeping Children Safe in Education 2018. *DfE, 2017*

Popular social media

74%

of 12-15 year olds have a profile on social media.

23%

of 8-11 year olds have a profile on social media.

32%

of 12-15 year olds say Snapchat is their main profile.

Source: Children and Parents: Media Use and Attitudes - Ofcom (2017)

Types of social media

There are so many ways for people to communicate online through various sites, apps and services. Below is a selection of the most popular apps and services used by children and young people.

Where available, pressing/clicking on the logos below will link you to the service's safety pages/ community guidelines.

Social networks

Facebook Instagram Snapchat Twitter Google+

Messengers

WhatsApp Messenger Kik Tango Viber Yubo

Video chat & livestreaming

Musical.ly Live.ly Periscope Skype FaceTime Google Hangouts Dubsmash

Blogging and content creation

YouTube Twitch Tumblr Reddit Pinterest

Popular social media

Risks

Communicating with others online provides many opportunities for young people to express themselves, gain and share ideas and make connections but it is also an area that can present risk in a number of forms. Historically these have fallen under the '4 Cs' but there is increasing evidence to suggest that social media can also affect young people's identity, mental health, wellbeing and self-esteem.

Contact	Content	Conduct	Commercialism
• Grooming • Contact from strangers • Cyberbullying • Trolling • Friendships/ Relationships • Sexual harassment • Cyberstalking	• Adult content • Extreme violent content • Extremist material • Child sexual abuse content • Inaccurate or unreliable content	• Sharing of personal information • Digital footprints & online reputation • Cyberbullying • Friendships/ Relationships • Sexual harassment • Sexting • Illegal behaviour	• Collection and use of personal information • Advertising • Gambling • Cybersecurity • Scams/phishing

Personal, Social, Health and Emotional

- Negative impact on mental health
- Low self-esteem
- Issues around body image
- 'FOMO' - Fear of missing out
- Peer pressure
- Problematic use/addictive behaviour
- Impact on academic achievement

13 is the minimum age for most social media services.

An explanation of age requirement legislation and advice you can give to children is provided in the section other legislation on the internet (page 23).

Resources for schools

- **NetAware** - The NSPCC's guide for parents/ teachers on the popular apps/services used by children.
- **Digital Literacy Curriculum** - Lesson plans and activities from SWGfL that cover a wide range of online behaviours, including social media use.

Resources for young people

- **h2b safer** - Resources by the INEQE Group that show how to use privacy settings and reporting tools on popular social media (sign up required.)
- **Social media checklists** - The UK Safer Internet Centre's checklists for privacy settings on Facebook, Twitter, Instagram and Snapchat.

Livestreaming

Definition

Livestreaming or 'going live' is the broadcasting of video live over the internet. It has been introduced on a number of social media services (such as Facebook, YouTube and Instagram) but there are also dedicated apps/services such as live.ly, Periscope, Meerkat and Twitch.

What are the benefits?

Broadcasting live video can be a very powerful way for someone to communicate with their friends or followers on social media. It gives celebrities and famous faces a chance to connect with their fans in a new way but also provides many opportunities for young people to share their thoughts, views and experiences or demonstrate their skills. It also provides chance for young people to be educators; through live tutorials, questions and feedback. And of course the occasional unplanned moments of silliness!

Risks

Livestreaming is not without its risks however and it is important make young people aware of these risks to ensure they can get the most out of going live.

The risks fall into two main types: risks you face when watching a livestream and risks you face when livestreaming yourself.

When watching a livestream:

- **Live** - All streams are live and in real time so you can never be sure what you will see.
- **Reliability** - Although live, it is not impossible for broadcasts to be manipulated or faked.
- **Commenting** - Comments posted on a live stream are seen by others (including the person/people in the broadcast) and could be offensive or upsetting or impact on people's reputations.

When going live:

- **Audience**- Depending on the app/service and the privacy settings, a livestream could be seen by a large audience, including strangers.
- **Personal information** - Details about a young person could be shared through what they say, how their appear on camera or other details captured by the broadcast (e.g. clues in the background).
- **Commenting** - Comments posted on a live stream are seen by others (including the person/people in the broadcast) and could be offensive or upsetting or impact on people's reputations.
- **Behaviour** - What is captured in the live stream will be seen by other people and may create an impression (positive or negative). Actions that break the law could also be captured.
- **Pressure or coercion** - Livestreaming to an audience can lead to expectations around behaviour or pressure to engage in risk taking to play up to the crowd.

How popular is it?

Over 1 in 10 young people have livestreamed.

Source: Young People's Experiences of Livestreaming - Childnet (2017)

LIVE Live streaming

Advice

It is important to reinforce messages around positive behaviour and managing risk for livestreaming in the same way as we discuss staying safe on social media in general:

- **Think before you share** - Whether it's a live broadcast, a verbal comment or a written comment, encouraging young people to be positive and thoughtful about their behaviour is key.
- **Remember it is live** - There is always the potential for unexpected things to happen in a live broadcast so young people should be prepared for this and recognise that their reaction will be seen immediately.
- **Commenting** - Other people may comment on a livestream and not all comments may be positive. Young people should be aware that they may receive critical or negative feedback depending on their actions and their audience.
- **Privacy settings** - As for other social media, privacy settings can be used to manage who can watch your livestream (both live and afterwards) and who can comment. Helping young people to explore and understand these tools will empower them to livestream more safely.
- **Peer pressure** - Young people need to remember that they always have the right to say 'no', can stop broadcasting or remove unwanted viewers and should never have to do anything on camera that makes them worried or uncomfortable.
- **Get help** - Reminding young people that they can always ask a trusted adult for advice, help and support is key. Knowing how to report a livestream or comments to the service provider is also important.

Resources for schools

- **#LiveSkills** - Teaching resources by CEOP that explore the features of livestreaming and the risks posed.
- **Video chat and webcams** - Advice from Childnet for professionals about the risks that young people face when videochatting.

Resources for young people

- **Top tips** - Tips and advice from young people for young people on positive livestreaming.
- **Video chat and webcams** - A Childnet factsheet for young people with advice on the risks around video chatting.

Further reading

- **Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse** - Research conducted by the IWF into the nature of abuse present in still images captured from livestreamed content. *IWF, 2018.*
- **Young People's Experiences of Livestreaming**- Research conducted by Childnet into the use and experiences of livestreaming by young people. *Childnet, 2017*
- **Livestreaming - What You Need to Know** - Information and advice from ParentZone and CEOP on the risks associated with livestreaming. *ParentZone, 2017*
- **Live.ly App – What parents need to know about the live streaming app** - Information from Internet Matters on live.ly and tips on how to help young people stay safe using it. *Internet Matters, 2018*

Cyberbullying

Definition

Cyberbullying (also known as online bullying) is bullying though the use of technology and the internet.

It can occur in many different ways such as nasty messages sent though social media or a messaging app, offensive comments under people's photos/videos, unkind behaviour in an online game (either through gameplay, messaging or audio chat) and other offensive electronic communication through email, phone calls, text messages etc. It can also be the distribution of images or videos (real or faked) to upset, worry or harass. It can also take the form of exclusion; where a young person is frequently left out of an online chat group or online game on purpose.

As with other forms of bullying, this behaviour is **deliberate and happens repeatedly**.

The effects

Bullying in any form can negatively impact on a child but 24/7 nature of online bullying means that it can have a huge impact on their wellbeing. It can lead to distress and worry, embarrassment, shame and a feeling of helplessness. In extreme cases it has resulted in self-harm and suicide.

Some signs a child is being cyberbullied may include:

- Low self-esteem
- Dramatic change of appearance or weight loss
- Withdrawal from social/family events
- Becoming secretive about devices and online accounts
- Friends/friendship group disappears
- Change in mood or personality
- Refusal to go to school

The Law

While there is no specific cyberbullying law in the UK, there are a number of other laws that relate to types of cyberbullying behaviour:

- The **Offences against the Person Act 1861** covers threats to kill.
- The **Protection from Harassment Act 1997** covers harassing behaviour.
- The **Malicious Communications Act 1988** covers communication that is 'indecent or grossly offensive' and sent with the 'intention of causing distress or anxiety'.
- The **Communications Act 2003** covers electronic communication that is of 'indecent, obscene or menacing character'.
- The **Computer Misuse Act 1990** covers behaviour where someone may hack into devices or online accounts.
- The **Defamation Act 2013** covers statements that cause or are likely to cause serious harm to the reputation of an individual or group.

Cyberbullying

Advice

It is imperative to know what to do if cyberbullying occurs, and to support young people to get help and a resolution to the issue.

The most important message is to **tell someone**, and to tell them sooner rather than later.

Advice for...

Young People	Parents/Carers	Staff and Schools
• Tell a trusted adult • Behave positively online • Look out for and support others • Keep personal info and accounts secure • Don't retaliate • Save the evidence (screenshots) • Use reporting and blocking tools	• Don't deny access to technology • Explore the apps/services your child uses • Talk with your child about cyberbullying • Become familiar with reporting tools on social media/games • Recognise that older children may not come to you first for help! • Know where to get further help/ support (e.g. school/police)	• Keep your eyes and ears open • Know your policies around bullying - do they adequately cover cyberbullying? • Record incidents and follow school procedures • Support all the young people affected • Education and prevention is key - take all opportunities to explore and discuss this topic

Resources for schools

- **Cyberbullying: Understand, Prevent and Respond**- Guidance from Childnet on ensuring cyberbullying incidents are managed effectively and positively.
- **Anti-Bullying Alliance** - Information and resources from the ABA, coordinators of Anti-Bullying Week in the UK.
- **MySelfie** - Teaching resources on cyberbullying for ages 10-12 from Irish charity WebWise.
- **Crossing the Line** - Childnet's PSHE Toolkit contains a film, lesson plan and activities on cyberbullying.

Resources for young people

- **StopSpeakSupport** - Information and advice from the Royal Foundation Taskforce on the Prevention of Cyberbullying.
- **Ditch the Label** - Advice and support from one of the world's largest anti-bullying charities.
- **Childline** - Advice and support for children and young people from the NSPCC.
- **Digizen Game** - A game created by Childnet to accompany the 'Let's Fight It Together' cyberbullying film.

Further reading

- **Amanda Todd Legacy Society** - Information, advice and support from a charity set up in memory of Amanda Todd, a US teen who took her own life after being cyberbullied in 2012.

Geolocation

Definition

Geolocation (also referred to as location based services) is the technology in modern mobile devices (smartphones, tablets, smart watches, etc.) that allows for that device's exact physical position on the planet to be determined, recorded, tracked and shared.

It is used frequently in apps that track location (e.g. Google Maps, Apple Maps, Find my iPhone, etc.) and is also used by a number of social media apps to permit more targeted advertising /content based on the device's geographical location, and to enable users to share their location with a message, photo or post (e.g. Facebook's Check In feature, Twitter, Instagram, etc.). Some social media apps allow real time tracking of other users e.g. Snapchat's Snap Maps feature).

What are the benefits?

Geolocation services can provide many useful functions and benefits, such as real time navigation on a map (smartphones have fast replaced dedicated GPS devices), location of missing or stolen devices (through service like Find my iPhone), and location of nearby services based on your location.

There also many recreational benefits such as being able to tag locations to photos, comments and messages on social media (to show where they were taken) and the rise of geocaching (the modern day equivalent of a treasure hunt using technology to locate hidden caches in the offline world). The functionality has been used in mobile games to enhance the experience and promote exploration of the physical world (e.g. augmented reality (AR) games such as Pokémon GO).

Risks

While sharing your location online or with an app can be fun, there are potential risks that need to be recognised and understood by young people in order to make well-informed choices on when it might be suitable to share their location, and with whom:

- Audience - On social media, the use of privacy settings affect who can see the location added to a photo or status update. Without privacy settings in place, the default setting may be to display this location to the public, allowing any user to see the activity and locations visited by a young person.
- Locations shared - While sharing a location when at a large venue/event (e.g. at a concert held at the O_2 arena) or significant landmark on holiday is unlikely to put personal safety at risk, a young person sharing locations that give away more information about routines or frequently visited locations (e.g. their house, their school, where they hang out on a Friday evening, etc.) could provide enough information for unwanted contact from strangers offline.
- Real time tracking - Features like Snap Maps can allow other users to be tracked in real time on a map, and for their exact position to be revealed. For young people, allowing any user to see this information
- Data collection - While collection of location data can enhance some of the apps and services we use, young people should be aware that their data is being collected by companies and must consider if they are happy with this to take place. Some mobile apps ask for permission to collect location data for no
- Meta data - Although less common now, some mobile devices automatically store location coordinates in the meta data of photos (data inside the file that gives details of the time and date, it was taken, what device it was taken on, etc). Most social networks remove this data from the photo when uploaded to their service, but photos uploaded to other sites (e.g. cloud storage) may still contain the data. This data can easily be extracted from the photo to give someone the exact location of the photo's origin.

Geolocation

Did you know?

47.9% of UK mobile users used location based services in 2017.

Source: Statista (2018)

Advice

It is important to make children and young people aware that their location can be recorded, tracked and shared across a variety of apps/services and to consider the following:

- What is shared - Encouraging young people to consider carefully which locations they share or tag on social media and what personal information is given away. As a general rule of thumb, if it is a location or information that would reasonably allow someone to locate you offline in the future, then it is probably best not to share it.
- Who gets to see - Reminding young people to consider their audience and who will be able to view the tag or location details is key. Using privacy settings gives control over whether the location is public, shared with friends/followers or completely private.
- Ghost Mode - On apps such as Snap Chat, enabling 'ghost mode' or turning off the display of real time tracking to other users is a useful way for young people to protect their location, activities and routines from being seen or tracked by strangers.
- Camera settings - Encourage young people to check the settings on their camera app to ensure that location data is not being collected in the meta data of the photos they take on their device.
- Data collection - Remind young people that the collection of their location data is used to improve their app experience but also to tailor advertising or generate revenue for the app provider. Encourage young people to consider this facto when deciding what apps to download and use.
- Check permissions - On most modern mobile devices, a prompt will appear to ask if the app can have permission to track location. Remind young people that they should only grant permission to the app if they are happy that it genuinely requires location data to work properly. If they have already given permission but want to prevent the app from access in the future, the permissions can be altered from the general settings of the device.

Professional reputation and safeguarding

The risks and advice outlined are also useful for staff members in order to maintain and manage their professional reputation. While sharing locations can be useful and beneficial, it is in the interests of your personal privacy to ensure that other members of the school community (e.g. pupils and parents/carers) cannot see your personal routines, activities or regular locales (e.g. home, where you like to eat out, where you might exercise, etc).

In the interests of safeguarding, it is highly recommended that staff responsible for school social media accounts (e.g. Twitter account, Facebook page) do not share locations related to offsite activities involving pupils e.g. sporting events, schools trips, residential trips.

More information on managing social media use as a school staff member can be found in **Childnet's 'Social Media Guide for Teachers and Support Staff'**.

Popular online games

66%

of 5-7 year olds play games, for nearly 7.5 hours per week.

81%

of 8-11 year olds play games, for around 10 hours a week.

77%

of 12-15 year olds play games, for around 12 hours a week.

Source: Children and Parents: Media Use and Attitudes - Ofcom (2017)

Information about popular online games

With games available on computers, dedicated games consoles (PlayStation, Xbox and Nintendo), smartphones and tablets, there is a wealth of content available for children and adults to explore and enjoy. As with social media, certain games and new releases trend in popularity, while some franchises regularly top the charts in terms of sales and popularity.

Therefore, this section aims to provide general information about online games, associated risks and links to regularly updated sources of information on current games and services that are popular with children and young people. A current (at the time of publication) popular game is also spotlighted, with additional links to information and advice.

Game spotlight: **Fortnite** 12 (PC, Xbox One, PS4, Switch, iOS)

© Copyright Epic Games

With an estimated 125 million players, Fortnite Battle Royale has captured the attention of children and adults alike with its competitive online matches involving 100 players at a time battling to be the last one standing. Matches last 20 minutes and becoming increasingly frenetic and exciting as the last few players fight for survival.

Violence is cartoony in nature (the game carries a **PEGI 12 rating**) and the game is free to play, although in-game transactions (V-Bucks) are available in order to buy cosmetic items such as skins (new outfits and looks for weapons) and the Battle Pass (a fast pass to earning rewards and unlocking new items more quickly).

Although each game is short, and there is a lot of potential for positive learning about communication and collaboration, many parents/carers have expressed frustration and worry over the amount of time that children are playing the game and how the competitive nature of the game and reward system makes it hard for children to disengage.
There are many sources of further information and advice on how to keep Fortnite a positive gaming experience in or out of home (the game was recently released on iOS devices):

Fortnite: all you need to know (NPSCC)
Parents' Ultimate Guide to Fortnite (Common Sense Media)
A parents' guide to Fortnite (UK Safer Internet Centre)
Fortnite Battle Royal parents' guide (Internet Matters)

Popular online games

Risks

Online gaming provides opportunities for many positive experiences, including entertainment and story telling, developing creative skills, problem solving, and communication/teamwork but it is also an area that can present risk in a number of forms. A brief summary of these risks are outlined below:

Contact	Content	Conduct	Commercialism
• Grooming • Contact from strangers • Cyberbullying • Trolling • Friendships/ Relationships • Sexual harassment • Cyberstalking	• Adult content • Extreme violent content • Extremist material	• Sharing of personal information • Online reputation • Cyberbullying • Friendships/ Relationships • Sexual harassment • Illegal behaviour	• Collection and use of personal information • Advertising • In-app purchases • Gambling • Cybersecurity • Scams/phishing

Personal, Social, Health and Emotional	
• Exposure to age restricted content can affect behaviour and well-being	• Peer pressure • Problematic use/addictive behaviour

PEGI ratings

All games sold in the UK for PC/Mac and video game consoles are rated by the Pan European Gaming Information service (PEGI). Apps on Google Play, Microsoft Store and Nintendo eShop are also given PEGI ratings. An explanation of the age rating and content descriptor labels can be found on the **PEGI website**.

Useful resources

- **AskAboutGames** - Information on PEGI ratings and family friendly games.
- **NSPCC's and O_2's NetAware** - A guide for parents/teachers on the popular apps/games used by children.
- **Online Gaming: An introduction for parents and carers** - A guide from Childnet on the risks around online gaming, with practical tips and advice.
- **Parents' Guide to Technology** - Advice about smartphones, gaming devices, tablets and other internet-connected devices, including where to find parental controls
- **Parental Control Guides** - Guides from Internet Matters for finding and setting parental controls (and privacy settings) on a wide range of devices and online services, including game networks.

Laws related to online behaviour

This section provides a summation of UK laws that apply to online behaviour. This information is provided for reference only and decisions around whether laws have been broken rest with the Police and the Crown Prosecution Service (England & Wales), the Crown Office & Procurator Fiscal Service (Scotland) and the Public Prosecution Service for Northern Ireland.

England & Wales

- Offences against the Person Act 1861 - It is an offence to make a threat to kill wherein the defendant intends the victim to fear it will be carried out.
- Protection from Harassment Act 1997 - Covers repeated bullying that amounts to harassment.
- Malicious Communications Act 1988 - It is an offence to send a communication with the intention of causing distress or anxiety.
- Communications Act 2003 Section 127 - It is an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character.
- Computer Misuse Act 1990 - An offence is committed in relation to unauthorised access to computer material, unauthorised modification of computer material and unauthorised access with intent to commit or facilitate further offences.
- Protection of Children Act 1978 - It is an offence to take, make, show, distribute, possess (with a view to distribute) or publish an advertisement with an indecent photograph or pseudo-photograph of a child under the age of 16. (Adjusted to under the age of 18 under the Sexual Offences Act 2003)
- Sexual Offences Act 2003 - It is an offence to meet or travel with the intention to meet a child following sexual grooming. Other sexual offences are also defined.
- Criminal Justice and Courts Act 2015 section 33 - It is an offence to share private sexual photographs or films with the intent to cause distress.
- Serious Crime Act 2015 section 67- From 3 April 2017, it is an offence to engage in sexual communication with a child.

Northern Ireland

- Offences against the Person Act 1861 - It is an offence to make a threat to kill wherein the defendant intends the victim to fear it will be carried out.
- Protection from Harassment (Northern Ireland) Order 1997 - Covers repeated bullying that amounts to harassment.
- Malicious Communications Act Order (Northern Ireland) 1988 - It is an offence to send a communication with the intention of causing distress or anxiety.
- Communications Act 2003 Section 127 - It is an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character.
- Computer Misuse Act 1990 - An offence is committed in relation to unauthorised access to computer material, unauthorised modification of computer material and unauthorised access with intent to commit or facilitate further offences.
- Protection of Children (Northern Ireland) Order 1978 article 3 - It is an offence to take, make, show, distribute, possess (with a view to distribute) or publish an advertisement with an indecent photograph or pseudo-photograph of a child under the age of 16. (Adjusted to under the age of 18 under the Sexual Offences Act 2003)
- Sexual Offences Act 2003 - It is an offence to meet or travel with the intention to meet a child following sexual grooming. Other sexual offences are also defined.
- Criminal Justice and Courts Act 2015 section 33 - It is an offence to share private sexual photographs or films with the intent to cause distress.

Laws related to online behaviour

This section provides a summation of UK laws that apply to online behaviour. This information is provided for reference only and decisions around whether laws have been broken rest with the Police and the Crown Prosecution Service (England & Wales), the Crown Office & Procurator Fiscal Service (Scotland) and the Public Prosecution Service for Northern Ireland.

Scotland

- Offences against the Person Act 1861 - It is an offence to make a threat to kill wherein the defendant intends the victim to fear it will be carried out.
- Protection from Harassment Act 1997 - Covers repeated bullying that amounts to harassment.
- Malicious Communications Act 1988 - It is an offence to send a communication with the intention of causing distress or anxiety.
- Communications Act 2003 Section 127 - It is an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character.
- Computer Misuse Act 1990 - An offence is committed in relation to unauthorised access to computer material, unauthorised modification of computer material and unauthorised access with intent to commit or facilitate further offences.
- Civic Government (Scotland) Act 1982 sections 52 and 52A - It is an offence to take, make, show, distribute, possess (with a view to distribute) or publish an advertisement with an indecent photograph or pseudo-photograph of a child under the age of 16.
- Breach of the Peace - A common law that can be used to prosecute any behaviour that causes fear or distress, including harassment and bullying.
- Abusive Behaviour and Sexual Harm (Scotland) Act 2016 - It is an offence to disclose publicly, or threaten to disclose publicly, an intimate photograph or film of another person in order to cause them distress.
- Sexual Offences (Scotland) Act 2009- It is an offence for an adult to knowingly send a sexual communication to a child.

Other legislation

- Digital Economy Act 2017 - Requires the Secretary of State to publish a code of practice for social media providers on responding to online bullying and harassment. Introduces an age-verification regulator to publish guidelines on how pornographic websites should ensure users are 18 or older and fine those who are non-compliant. Raises maximum sentence for internet copyright infringement (e.g. piracy) to 10 years in prison.
- Defamation Act 2013 - Makes a website host responsible for removing defamatory material posted on their site/service.
- Education Act 2011 (England only)- Provides schools and staff with powers to search for, confiscate and destroy/delete materials or data that is against school rules or constitutes a banned substance/object (e.g. bullying content, pornography, knives, drugs, etc.)
- General Data Protection Regulation (GDPR) - From 25 May 2018, this legislation around date protection introduces a greater need for data controllers (websites, services, companies) to show greater transparency around how data is collected, used and stored, as well as actively seeking consent for data collection, storage and use. These duties extend to schools as they are also a data controller. Article 8 introduces a minimum age of 16 for children to consent to the processing of their data. EU member states can choose to set a different minimum age (between 13 and 16) and the UK has opted for a minimum age of 13. This will have impact on how social media services may verify that children meet the age of consent when signing up/continuing to use their services.
- Children Online Privacy Protection Act (COPPA) (USA only) - COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

Developing policy and practice for schools

Safeguarding children online is dependent not only on education but effective and impactful school practice, as well as regard for statutory guidance and legislation.

Below is an overview of guidance and frameworks that provide advice and guidance for developing good practice towards online safety and safeguarding. (Please note that some only apply to schools in England).

Department for Education

Keeping children safe in education (2018)

Schools and colleges/governors and proprietors...

- ...**should ensure** children are taught about safeguarding, including **online safety**, through teaching and learning opportunities, as part of providing a broad and balanced curriculum...
- ...should ensure **appropriate filters and appropriate monitoring systems** are in place...
- ...should consider a **whole school approach** to online safety. This will include a **clear policy on the use of mobile technology in the school**. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises...
- ...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.
- ...should ensure...that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Designated Safeguarding Leads (DSLs)...

- ...are able to understand the **unique risks associated with online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college...
- ...can recognise the **additional risks that children with SEN and disabilities (SEND) face online**, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online...

Sexual violence and sexual harassment between children in schools and colleges (2017)

- Sexual violence and sexual harassment exist on a continuum and may overlap, they **can occur online and offline** (both physically and verbally) and are never acceptable.
- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
  - non-consensual sharing of sexual images and videos. (UKCCIS sexting advice provides detailed advice for schools and colleges);
  - sexualised online bullying;
  - unwanted sexual comments and messages, including, on social media; and
  - sexual exploitation; coercion and threats.
- Schools and colleges should recognise that sexual violence and sexual harassment occurring online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across **a number of social media platforms and services**, and for things to **move from platform to platform** online. It also includes the potential for the impact of the incident to **extend further than a schools or college's local community** (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become **marginalised and excluded** by both online and offline communities. There is also the strong potential for **repeat victimisation** in the future if abusive content continues to exist somewhere online.
- **Social media** is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could harass the victim or alleged perpetrator online and/or become victims of harassment themselves.

Developing policy and practice for schools

Welsh Government

Digital Competence Framework (updated 2018)

- Focuses on developing digital skills which can be applied to a wide range of subjects and scenarios.
- Has 4 strands of equal importance, each with a number of elements.
  - Citizenship – which includes:
    - Identity, image and reputation
    - Health and well-being
    - Digital rights, licensing and ownership
    - Online behaviour and cyberbullying.
  - Interacting and collaborating – which includes:
    - Communication
    - Collaboration
    - Storing and sharing.
  - Producing – which includes:
    - Planning, sourcing and searching
    - Creating
    - Evaluating and improving.
  - Data and computational thinking – which includes:
    - Problem solving and modelling
    - Data and information literacy.

Scottish Government

National Action Plan on Internet Safety for Children and Young People (2017)

- The Scottish Government will work to ensure children and young people are supported to build their own resilience online.
- Education Scotland will support local authorities in implementing the new Technologies Curriculum guidance, which has a specific focus on digital literacy.
- Education Scotland will ensure inspectors are aware of the expectation to deliver education that encourages innovation, confidence and responsibility in the use of technologies and staying safe online.
- The Scottish Government and Education Scotland will work with the South West Grid for Learning to promote and update the **360 degree safe tool**.
- Education Scotland will work with **Digital Schools Awards Scotland** to develop a link to relevant resources on internet safety for children and young people.
- The Scottish Government will consider what resources are available within youth work organisations on internet safety and whether more can be done to build on and amplify good practice, for consistency, with resources available across Scotland.
- The Scottish Government will consider the findings of the Youth Commission in future policy development. Working with partners, the Scottish Government will promote the principles of the movement to inform citizens of the **5rights**.
- The Scottish Government will continue to engage with disabled people's organisations across Scotland to better understand the needs of disabled children and young people in the online world in order to ensure the most effective training, information and support is in place.

South West Grid for Learning (SWGfL)

360 Degree Safe - A free online safety self-review tool for schools with optional accreditation.

- Available for **England (360safe.org.uk)**, **Wales (360safecymru.org.uk)** and **Scotland (360safescotland.org.uk)**.

Online Compass - An alternative to 360 Degree Safe aimed at other groups/settings that work with children and young people.

360 Degree Data - Online data protection self-review tool.

Developing policy and practice for schools

UK Council for Child Internet Safety (UKCCIS)

Education for a Connected World (2018)

A framework that describes the digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

The document supports one of the key aims of the government's Internet Safety Strategy of supporting children to stay safe and make a positive contribution online, as well enabling teachers to develop effective strategies for understanding and handling online risks.

Sexting in schools and colleges (2017)

The UKCCIS Education Group has produced advice for schools and colleges on responding to incidents of 'sexting.' The advice aims to support them in tackling the range of issues which these incidents present including responding to disclosures, handling devices and imagery, risk assessing situations and involving other agencies. The advice also contains information about preventative education, working with parents and reporting imagery to providers. This advice is non-statutory and should be read alongside the Department for Education's **Keeping Children Safe in Education** statutory guidance and non-statutory **Searching, Screening and Confiscation** advice for schools.

- For Welsh schools - A version of the advice is available in **English** and **Welsh**. This advice is non-statutory and should be read alongside the Welsh Government's **Keeping learners safe** statutory guidance.

Using External Visitors to Support Online Safety Education (2017)

Educational settings seeking support from external visitors to help explore issues such as cyberbullying, online pornography, 'sexting' and staying safe online can use this document to guide their process of selecting suitable visitors and sessions. This consultation document explores key questions in the form of a checklist to help educational settings ensure the maximum impact of online safety sessions. The guidance highlights a range of resources which can be used to support educational settings to develop a whole setting approach towards online safety in line with national guidance. The document can be used to facilitate conversations between educational settings and external visitors to develop children and young people digital literacy skills and parental awareness.

Online safety in schools and colleges: Questions from the Governing Board (2016)

The UKCCIS Education Group has developed guidance for school governors to help governing boards support their school leaders to keep children safe online. Governors can use it to: gain a basic understanding of the school's current approach to keeping children safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. The document includes examples of good and outstanding practice, as well as identifying when governors should be concerned. This guidance is non-statutory and should be read alongside the Department for Education's **Keeping Children Safe in Education** statutory guidance.

UK Safer Internet Centre

Appropriate filtering and monitoring

The UK Safer Internet Centre provides documents for schools and service providers on what should be considered as 'appropriate' filtering and monitoring. Providers can self-certify their systems and display their response on the site to show schools that they are compliant with the requirements laid out in **Keeping Children Safe in Education** and the **Revised Prevent Duty Guidance: for England and Wales (2015)**.

Information for parents/carers

CEOP Command: The National Crime Agency's CEOP Command tackle child sexual abuse and exploitation online. The website includes the **Click CEOP** report button that allows both adults and young people to make reports of actual or attempted abuse online. **www.ceop.police.uk**

CEOP's **Think U Know** site contains information for children of all ages, as well as parents/carers. **www.thinkuknow.co.uk**

Childnet International: A non-profit organisation working in partnership with others around the world to help make the internet a great and safe place for children. The Childnet website has a range of resources for young people, parents/carers and adults who work with children. **www.childnet.com**

A Parents and Carers section with key information and advice about online risks. **www.childnet.com/parents-and-carers**

A template Family Agreement and conversation starters to help families discuss online safety. **www.childnet.com/have-a-conversation**

Common Sense Media: A US not-for-profit organisation that offers information and advice for parents/carers around digital content. They regularly review films, TV shows, games, apps and websites to provide suggestions of what is suitable for different ages. **www.commonsensemedia.org**

Digital Parenting: An online magazine, created by **Parentzone** and the **Vodafone Foundation**, with articles and expert advice for parents and educators on a range of topics related to the digital world. **www.vodafonedigitalparenting.co.uk**

Internet Matters: A not-for-profit organisation backed by the UK's main internet industry companies that provides information, advice and guides for parents/carers on how to keep children safe online. **www.internetmatters.org**

Over 70 step-by-step guides for enabling parental controls on devices, entertainment services and networks as well as privacy settings on popular social media services. **www.internetmatters.org/parental-controls**

NSPCC: If you have questions about parental controls or concerns about a child's online safety then you contact the Online Safety Helpline run by the **NSPCC** and **O2** on **0808 800 5002**. **www.nspcc.org.uk**

Children can talk to someone for advice and support at any time by contacting **Childline** on **0800 1111** or chatting to a counsellor online at **www.childline.org.uk**.

A guide to what parents/carers need to know about the social networks and games their children use. **www.net-aware.org.uk**

Practical information, advice and videos for parents and carers to encourage their children to be Share Aware online. **www.nspcc.org.uk/share-aware**

UK Safer Internet Centre: Appointed by the European Union, the UK Safer Internet Centre raises awareness about online safety, develops resources and organises high profile events such as Safer Internet Day. **www.saferinternet.org.uk**

A free Parents' Guide to Technology that gives information and advice on how to set up smartphones, gaming devices, tablets and Smart TVs for children to use. **www.saferinternet.org.uk/parent-tech**

Free Social Network Checklists for privacy settings on Facebook, Twitter, Instagram and Snapchat. **www.saferinternet.org.uk/checklists**

The Parents/Carers pack for Safer Internet Day contains lots of useful information and advice about online safety. **bit.ly/SID2018Parents**

Where to get help

For **online safety issues** involving children/young people or school staff:

Professionals Online Safety Helpline

Run by the **UK Safer Internet Centre**, the helpline supports all professionals working with children and young people. They can help with any online safety issue and have direct channels to escalate concerns to social media companies and many websites.

Email: **helpline@saferinternet.org.uk**

Tel: **0344 381 4772** (Mon-Fri, 10am-4pm)

For reporting **online grooming/sexual abuse**:

CEOP

CEOP command of the National Crime Agency are dedicated to tackling child sexual abuse and exploitation. The 'Make a report' button allows young people and adults to report actual or attempted abuse and online grooming

www.ceop.police.uk

For reporting **child sexual abuse images:**

IWF Internet Watch Foundation

While it is rare to stumble across child sexual abuse content when browsing the internet in the UK, it is still possible to see such material. If you do see content of this nature, you can report it to the **Internet Watch Foundation**, the UK hotline for reporting child sexual abuse content.

www.iwf.org.uk

For reporting **online material promoting terrorism or extremism:**

GOV.UK

A page run by the **Home Office** for reporting illegal or harmful information, pictures or videos found online. Reports can be made anonymously.

www.gov.uk/report-terrorism

For reporting offline or online **hate crimes:**

TRUEVISION

A page run by the **National Police Chiefs' Council** for leaning about and reporting homophobic, transphobic, race, religious and disability hate crimes.

www.report-it.org.uk

For making a complaint about **unsuitable media content:**

PARENT PORT WORKING TOGETHER FOR MEDIA STANDARDS

Run by the UK's media regulators, **ParentPort** provides information and ways to make a complaint about something unsuitable for children on TV or online, in films, adverts, video games and printed media.

www.parentport.org.uk

HOW DO WE PREVENT CHILD SEXUAL ABUSE?

I always thought he/she was odd...!

This is what many people say to us after an abuser has been exposed. They fear being a whistle blower unless they are truly certain. Our education is designed to give people confidence about what they are seeing and sensing and so act to protect children in their care having identified a risk.

Our founder, Marilyn Hawes, experienced this situation, she trusted the head teacher, who was her boss and best friend, and sadly her three boys were sexually groomed and abused by him. Marilyn did not wish other families and schools to suffer and has successfully delivered this education since 2004.

The education is based on respected research and personal experience making our program unique, memorable and proven to be effective. We now offer education across **all** sectors in the UK and abroad.

Our education programs focus on prevention**,** enabling delegates to understand how abusers think and function, meaning they can identify a potential abuser from their **grooming** behaviours.

Additionally, we train children as young as seven on how to protect themselves **online and offline**, how abuse feels, and how to report it, thereby reducing the awful impact of this harm.

Nelson Mandela said:

"THE TRUE CHARACTER OF A SOCIETY IS REVEALED IN HOW IT TREATS ITS CHILDREN".

For more information and to enquire about how we can work with your school/setting, please contact **Roger** at **roger.woods@ff-a.uk** or **ff-a.uk/contact/**

Contact us

freedom from abuse

For enquiries about training:

Roger Woods - roger.woods@ff-a.uk or ff-a.uk/contact/

For press/media enquiries:

Marilyn Hawes, CEO - marilyn.hawes@ff-a.uk

For feedback/questions about 'The Digital Generation':

Gareth Cort, Director - gareth.cort@ff-a.uk

Freedom from Abuse C.I.C.

Registered in England and Wales. Company No. 11218440

freedom from abuse

www.ff-a.uk

@freedom_abuse