Safeguarding Spotlight

Cybercrime, Online Safety & Gaming

The 4 main risks to children in terms E safety are:

The 4 C's

o **Content** – being exposed to illegal, inappropriate or harmful material

o **Contact** – being subjected to harmful online interaction with other users

o **Conduct** – personal online behaviour that increases the likelihood of, or causes harm

o **Commerce -** risks such as online gambling, inappropriate advertising, phishing and or financial scams

The 4 Cs place increased risk on users because:

o Younger children becoming vulnerable to this form of online abuse.

o Loss of control over content – it can be harvested from the original broadcast service (Facebook, Instagram etc) and then misused / shared / manipulated.

o Children can be blackmailed and coerced to produce more severe material than they want to share.

o Children lack an awareness of the potential permanence of imagery captured from live streams.

o Increased commercialisation of captures of live-streamed child sexual abuse.

o Since the start of the pandemic, the amount of 'self-generated' child abuse imagery has increased dramatically.

Video (1 min)

- TALK Checklist by Internet Watch Foundation | Home (iwf.org.uk)

Live Streaming and indecent images (the internet watch foundation (IWF)

o Live streaming -dangerous offenders are capitalising on the immediacy of contact that live streaming offers. They often use tricks or dares, the offer of online gifts or 'game points' and threats, in an attempt to manipulate young people into performing acts involving nudity over webcam.

o Youth-produced Sexual Imagery, Self-Generated Child Sexual Abuse Material or Sexting has increased

o Naked or semi-naked images or videos created by a child or young person depicting sexual activity. Which may be shared consensually and forwarded or obtained maliciously by offenders and uploaded to other sites.

o Last year, the IWF took action against 252,000 URLs which contained images or videos of children being raped and suffering sexual abuse.

o Adults can also report the URL of images for removal directly to the Internet Watch Foundation.

Knowing how to remove an image on the internet
'Report Remove'

Video (1 min)

Report Remove | Remove a Nude Image Shared Online | Childline – YouTube

Sharing nudes and semi-nudes

- **London Grid for Learning-collection of advice** - Various information and resources dealing with the sharing of nudes and semi-nudes;

- **UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people** - Advice for schools and colleges on responding to incidents of non-consensual sharing of nudes and semi-nudes.

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either:

- **'cyber-enabled'** - crimes that can happen off-line but are enabled at scale and at speed on-line

- **'cyber dependent'** - crimes that can be committed only by using a computer.

Cyber-dependent crimes include:

- Unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;

- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and

- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above

- Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

- If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the **Cyber Choices** programme.

- This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

- Note that **Cyber Choices** does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

- Additional advice can be found at: **Cyber Choices**, '**NPCC - When to call the Police**' and **National Cyber Security Centre - NCSC.GOV.UK**.

The Dark web explained

Video (5 mins)

- [The Dark Web Explained (thinkuknow.co.uk)](#)

Deep Fakes explained

Video (2.5 mins)

- [Deepfake generators Wombo, MyHeritage and Avatarify are booming without many guardrails - The Washington Post](#)

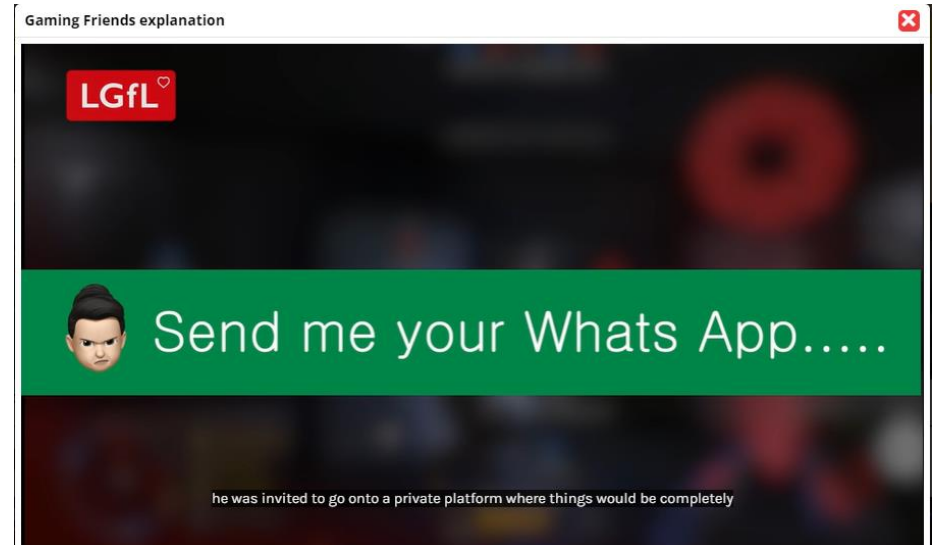# Gaming

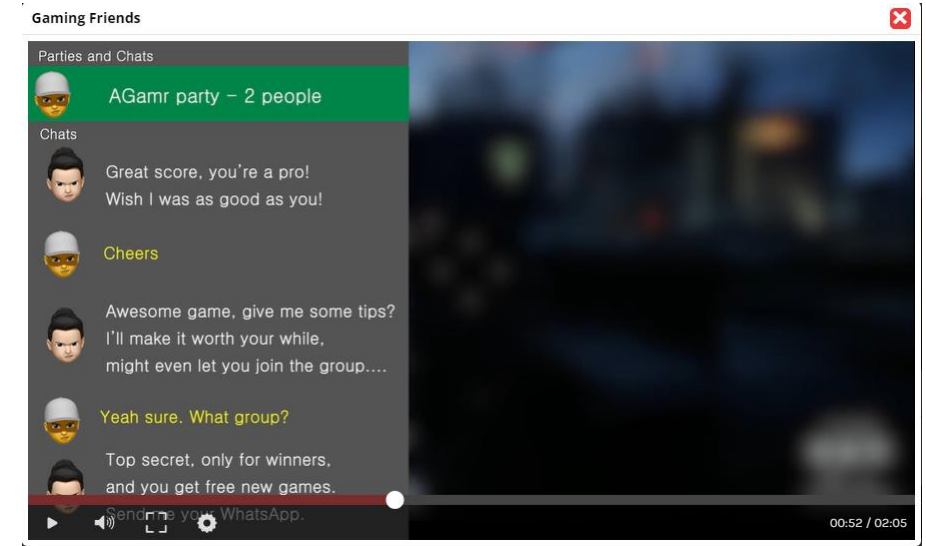**Link to video: Gaming Friends (2 mins)**

- Going Too Far? (lgfl.org.uk)

Link to video: Teachers Guidance

(3 mins) Optional

- Going Too Far? (lgfl.org.uk)

Digital Resilience

o Given that young people will inevitably use digital technologies and be exposed to negative online experiences, it is vital to find ways to protect them that don't unduly limit their access or undermine the positive outcomes of internet use

o In addition to raising awareness about online risks and increasing online protection, we need to support young people to build their own digital skills and resilience, so they can navigate online

o We also need to educate parents so they can support their children

Watching online videos

- 91% of 5-15 year olds watch videos online

- Inappropriate content

- Sexual images

- Violent behaviour

- Encourage crime, self harm or suicide

Video Parent Guide (2.57mins)
- [Guide to watching online videos - YouTube](#)

Online safety - Parental support

- **Childnet** offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support;

- **Commonsensemedia** provide independent reviews, age ratings, & other information about all types of media for children and their parents;

- **Government advice** about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying;

- **Internet Matters** provide age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world;

- **How Can I Help My Child?** Marie Collins Foundation - Sexual Abuse Online;

- **Let's Talk About It** provides advice for parents and carers to keep children safe from online radicalisation;

- **London Grid for Learning** provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online;

- **Stopitnow** resource from **The Lucy Faithfull Foundation** can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online);

- **National Crime Agency/CEOP Thinkuknow** provides support for parents and carers to keep their children safe online;

- **Net-aware** provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games;

- **Parentzone** provides help for parents and carers on how to keep their children safe online;

- **Talking to your child about online sexual harassment: A guide for parents** – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment;

- **#Ask the awkward** – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships.

Online safety - advice

- **Childnet** provide guidance for schools on cyberbullying;

- **Educateagainsthate** provides practical advice and support on protecting children from extremism and radicalisation;

- **London Grid for Learning** provides advice on all aspects of a school or college's online safety arrangements;

- **NSPCC E-safety for schools** provides advice, templates, and tools on all aspects of a school or college's online safety arrangements;

- **Safer recruitment consortium** "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective;

- **Searching screening and confiscation** is departmental advice for schools on searching children and confiscating items such as mobile phones;

- **South West Grid for Learning** provides advice on all aspects of a school or college's online safety arrangements;

- **Use of social media for online radicalisation** - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq;

- **Online Safety Audit Tool** from UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring;

- **Online safety guidance if you own or manage an online platform** DCMS advice **A business guide for protecting children on your online platform** DCMS advice;

- **UK Safer Internet Centre** provide tips, advice, guides and other resources to help keep children safe online.

Online safety - Remote education, virtual lessons and live streaming

- **Case studies** for schools to learn from each other;

- **Guidance Get help with remote education** resources and support for teachers and school leaders on educating pupils and students;

- **Departmental guidance on safeguarding and remote education** including planning remote education strategies and teaching remotely;

- **London Grid for Learning** guidance, including platform specific advice;

- **National cyber security centre** guidance on choosing, configuring and deploying video conferencing;

- **UK Safer Internet Centre** guidance on safe remote learning.

Online Safety - Support for children

- **Childline** for free and confidential advice;
- **UK Safer Internet Centre** to report and remove harmful online content;
- **CEOP** for advice on making a report about online abuse.