University of East London

ICC
THE INSTITUTE FOR CONNECTED COMMUNITIES

CHILD ONLINE HARMS POLICY THINK TANK

Online Risks and Harms to Children

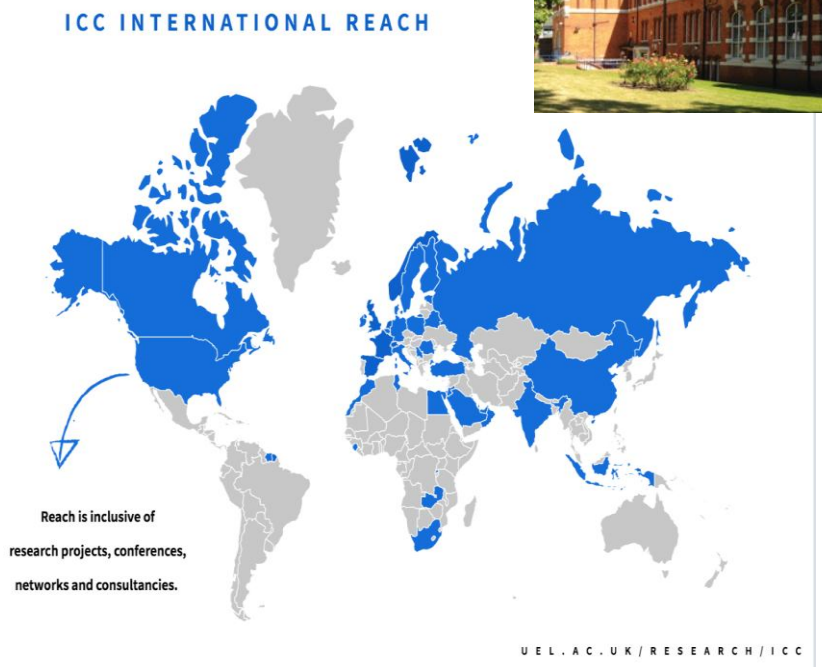
National Council for Child Health & Wellbeing, 9th July 2025

Professor Julia Davidson OBE, PhD(LSE),
Director Institute for Connected Communities,
UEL.

ICC@uel.ac.uk

UEL Institute for Connected Communities

- Interdisciplinary research institute, established for 4 years as ICC (10 years ad IHHD) - world leading researchers
- Youth cybercrime, online harms and safety health and wellbeing: Sociology, criminology, psychology & cyberpsychology, law and public health.
- Local, national and international focus: UK, Africa, India, Middle East, US & EU.
- Tradition of delivering community-based health and safety initiatives – real world and digital
- Broad approach to CYP safeguarding – evidence based
- 20 million plus in research funding- diverse sources



- https://www.uel.ac.uk/our-research/research-school-education-communities/institute-connected-communities-icc

University of East London

ICC
THE INSTITUTE FOR CONNECTED COMMUNITIES

Our Research Impact - Online Harms & Safety Tech

University of East London

INSTITUTE FOR CONNECTED COMMUNITIES

Research on Protection of Minors:
A Literature Review and Interconnected Frameworks. Implications for VSP Regulation and Beyond

Professor Julia Davidson, *Co-Lead*
Professor Mary Aiken, *Co-Lead*
Dr Anna Gekoski, *Research Fellow*
Kirsty Phillips, *Research Assistant*
Ruby Farr, *Research Assistant*

REPHRAIN
Protecting citizens online

European Online Grooming Project_

Press release

New report reveals UK as world leader in online safety innovation

The UK's rapidly-growing safety tech sector is helping make the online world safer for millions of people, a report published today shows.

From: Department for Digital, Culture, Media & Sport and Caroline Dinenage MP
Published 27 May 2020

HORIZON 2020

CC-DRIVER

Framework of Benefits OFCOM (2020 Davidson et al)

Broad category of benefit	*Specific benefits*
Knowledge	Information Education Learning Health advice/support
Connection	Friendships/relationships Staying connected Building social capital Reducing loneliness Emotional support/belonging
Enjoyment	Entertainment Fun Exploration Play
Expression	Creativity Self-expression Self-identity

What does our original research tell us about Technology use when it comes to children and young people? (Davidson et al, 2019, OFCOM)

Identified Benefits

- Information, Education and Learn
- Entertainment, Fun, and Creativity
- Self-expression and Self-identity
- Friendships, relationships, and staying connected
- Building Social Capital and Reducing Loneliness
- Emotional Support and Belonging
- Health Advice, Information, and Support

How are Children Harmed Online?

NSPCC
Cruelty to children must stop. FULL STOP.

Risk does not equal harm

The likelihood of harm is dependent upon a number of factors including:

-Age

-Vulnerability

-Type of risk

-Length of exposure to risk

-Protective factors

Risky Pathways Model (Gill, 2022)

- **Isolated exposure to hazards that have immediate but largely transient emotional impacts, leading to minimal harm**
- **Cumulative passive exposure to hazards over time can lead to more significant harm**
- **Cumulative active engagement refects longer-term engagement with content and contact that self-reinforces attitudes or behaviours, (can)lead to significant and severe harm eg longer term grooming**

Online Harms

- **Cyberbullying:** emotional harassment, defamation and social exposure, intimidation, social exclusion, hate
- **Cyber extremism/radicalisation:** ideological indoctrination and recruitment, threats of extreme violence
- **Online sexual abuse & exploitation:** distribution of sexually explicit and violent content (can be self generated), sexual harassment, online grooming, production, distribution and use of child sexual abuse material , “sextortion”.
- **Online crime** e.g hacking and financial crime as victims and perpetrators
- **Exposure to Harmful content** : Children’s role?

  Sharing illegal content

Framework of Risk and Harm (OFCOM. Davidson et al 2020)

Sexual	• Pornography • Sexting • Naked selfies/nudes • Grooming • Child sexual abuse • Child sexual exploitation-/-coercion • Child sexual abuse materials • Livestreaming of child sexual activity/abuse • Meeting online strangers in real life
Aggression	• Hate speech • Violence/Incitement to violence • Extreme content • Cyberbullying • Online harassment • Cyberstalking
Manipulation	• Image/video filtering, editing and photoshopping • Fake profiles • Fake news • Mis/disinformation • Deep fakes • Radicalisation • Profiling • AI and algorithmic manipulation • Persuasive design, nudging and targeting
Self-injurious	• Exposure to self-harm • Exposure to eating disorders • Exposure to suicide content • Exposure to alcohol and tobacco

Mental health/ wellbeing	• Psychological distress • Depression • Anxiety • Loneliness • Isolation • Social withdrawal • Low self-esteem/inadequacy • Fear of Missing Out (FOMO) • Addictive type behaviours • Problematic Internet Use • Gaming disorder
Cognitive	• Attention • Memory • Executive function • Brain structure/functioning
Moral	• Judgement • Decision-making • Character traits • Values
Physical	• Sleep deprivation • Obesity • Tech ergonomic risk
Cyber deviance	• Identity theft • Hacking • Cyberscams/Cyberfraud • Malware/Spyware

Who is Vulnerable Online?

Some children appear to be specifically 'at risk' online, being either more likely to encounter risk or when they do encounter risk, more likely to find it harmful. In short, they may be less resilient or less able to cope'

Livingstone, Davidson & Bryce, p69, 2017

Complex issue:

- **Children who experience family difficulties** or who are brought up in chaotic family/home environments they may suffer physical, emotional and/or sexual abuse and neglect, witness domestic violence and/or family breakdown,
- **Children with disabilities -** they may suffer from chronic physical ill health, have physical or learning disabilities
- **Children with emotional/ behavioural difficulties -** these children may present with differing symptoms;
- **Children who experience exclusion of access -** these children experience system neglect - more marginalised groups within society such as travellers, asylum seekers, trafficked and migrant communities

(Finkelhor et al , 2018, 2020, 2023)

Children as Perpetrators of Cybercrime

- H2020 – CcDriver - Drivers of Cybercriminality . EC grant , 8 million Euros
- 8 EU countries, 14 partners – criminology, psychology, law, computer science, health, education & police partners. Led by Trilaterial research
- Explore drivers and develop tech and non tech prevention programmes
- UEL (1 million euros) – Davidson & Aiken – youth pathways into cybercrime , online national youth surveys in 8 countries
- Largest survey youth cybercrime- 8000 YP in 8 countries

CC-DRIVER

CC-DRIVER

- Drivers of Cybercrime. Our focus- youth Cyber crime. H2020 call referred to our original EC3 research.
- UEL's focus- exploring youth cybercrime (human and technical factors and motivations)

Methods

- ✓ Literature and expert review of cyber juvenile delinquency and criminality
- ✓ Exploration of cybercrime definitions
- ✓ Interview studies with cybercrime experts (N=36)
- ✓ Panel/Quota Sample (n= 7974) youth 18-22– Self-report online survey consisting of approx. 1,000 respondents in 7 EU countries and one region (U.K, France, Spain, Italy, Germany, Romania, Netherlands, Norway & Sweden).
- ✓ Interviews with convicted cybercrime offenders (N=12) – UK and Swiss jurisdictions
- ✓ Outputs: Evidence-based educational, awareness and intervention programmes for EU and online safety networks; Policy recommendations and briefs

CCDriver Youth Cybercrime Survey - Summary Points

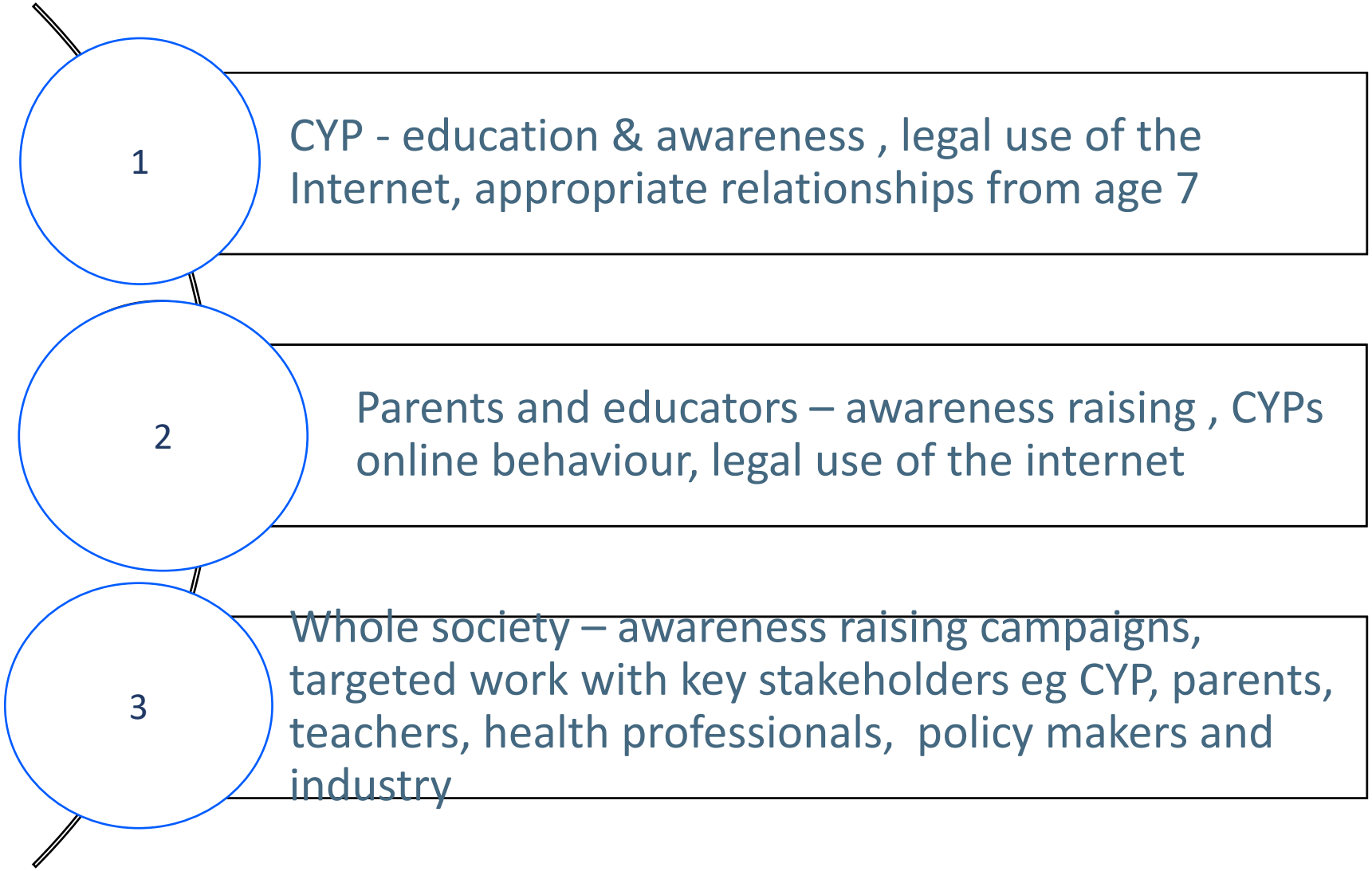
- Youth surveyed (N=7974) **are immersed in technology** & most connected generation to date
- Large majority of youth surveyed (69.1%, N=5507) engaging in some form of **online risk taking or cybercriminality**
- Just under half 47.76% (N=3808) report to have engaged in **criminal behaviour online (majority low level crime)**
- **Prevalence rates** for cyberdeviant/cybercriminal behaviours measured range from approx. 1 in 2 to 1 in 13
- Broadly there are differences in cyberdeviant/cybercriminal behaviours across gender, age and country
- Findings inform **evidence-based** education and awareness, and intervention initiatives

Offending rates

- 1 in 3 report to have engaged in digital piracy (2702 33.9%)
- 1 in 4 have trolled someone else online (2124 26.6%)
- 1 in 5 have engaged in sexting (1727 21.7%)
- 1 in 7 have produced self-generated sexual images (1118 14.9%)
- 1 in 8 have engaged in money muling/laundering (982 12.3%)
- 1 in 8 have engaged in online harassment (969 12.2%)
- 1 in 10 have engaged in hate speech (872 10.9%)
- 1 in 10 have engaged in hacking (859 10.8%) or cyberbullying (804 10.1%)
- 1 in 11 have engaged in phishing (726 9.1%), non-consensual sharing of intimate images (707 8.9%), cyberfraud (696 8.7%), identify theft (676 8.5%) or online racist/xenophobic speech (721 9%)
- 1 in 13 have engaged in sextortion online (621 7.8%)

Youth Cybercrime Primary Prevention

PREVENTION



Online Safety Act 2023

Protect children online by making social media platforms and content providers (VSPs etc):

- Began life as Online Harms Bill
- remove illegal content quickly or prevent it from appearing in the first place. This includes removing content promoting self harm
- prevent children from accessing harmful and age-inappropriate content
- enforce age limits and age-checking measures
- ensure the risks and dangers posed to children on the largest social media platforms are more transparent, including by publishing risk assessments
- provide parents and children with clear and accessible ways to report problems online when they do arise
- Platforms will also have a duty to report any child sexual exploitation and abuse content that they encounter to the National Crime Agency

Harmful Content

Some content is not illegal but could be harmful or age-inappropriate for children. Under the OSA Platforms must prevent children from accessing it.

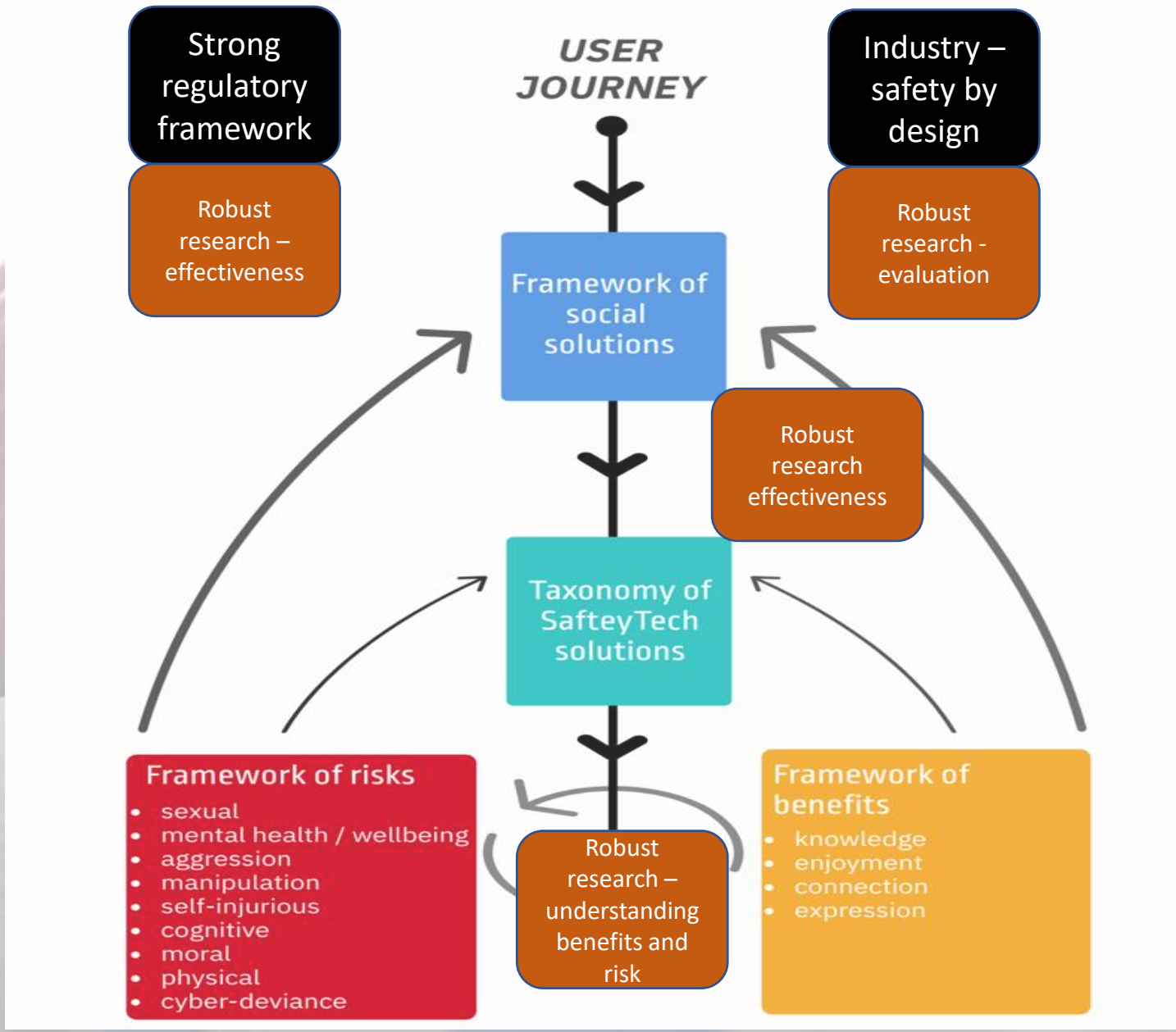
- Harmful content that platforms will need to protect children from accessing will include:
- pornographic content
- online abuse, cyberbullying or online harassment
- content that does not meet a criminal level but which promotes or glorifies suicide, self-harm or eating disorders

Enforcement

- Ofcom is the Regulator.
- Platforms will have to show they have processes in place to meet the requirements set out by the Act.
- Must complete risk assessments annually
- Ofcom will monitor effectiveness and will have powers to take action against companies which do not follow their new duties.
- Companies will be fined up to £18 million or 10 percent of their annual global turnover, whichever is greater.
- Criminal action may be taken against senior managers who fail to follow information requests from Ofcom.
- In the most extreme cases, with the agreement of the courts, Ofcom will be able to require payment providers, advertisers and internet service providers to stop working with a site, preventing it from generating money or being accessed from the UK.

Whole systems approach to safeguarding

OFCOM- Davidson et al 2021



Key Issues

- Children benefit from the Internet and their experience is largely positive
- Can experience a range of harms including sexting, cyberbullying, online grooming/solicitation, trolling, revenge porn
- Some children and young people are more vulnerable online – awareness, prevention and support.
- URCRC has been updated to include children's online rights
- The OSA must deliver on online safety for children
- Contentious issues focus on legal but harmful (adults) and penalties for non-compliance
- OSA is a legal milestone – attempts to regulate social media industry for the first time, important to place in wider context of social and tech approaches.
- Challenge will be for OFCOM in defining ‘harm’, enforcement and monitoring compliance.

ICC Outputs & Resources

-Toolkit Report

-Blogs and media reporting

-Two peer reviewed journal articles on our findings.

-A webinar attended by professionals and practitioners: Presentation of findings at conferences and seminars

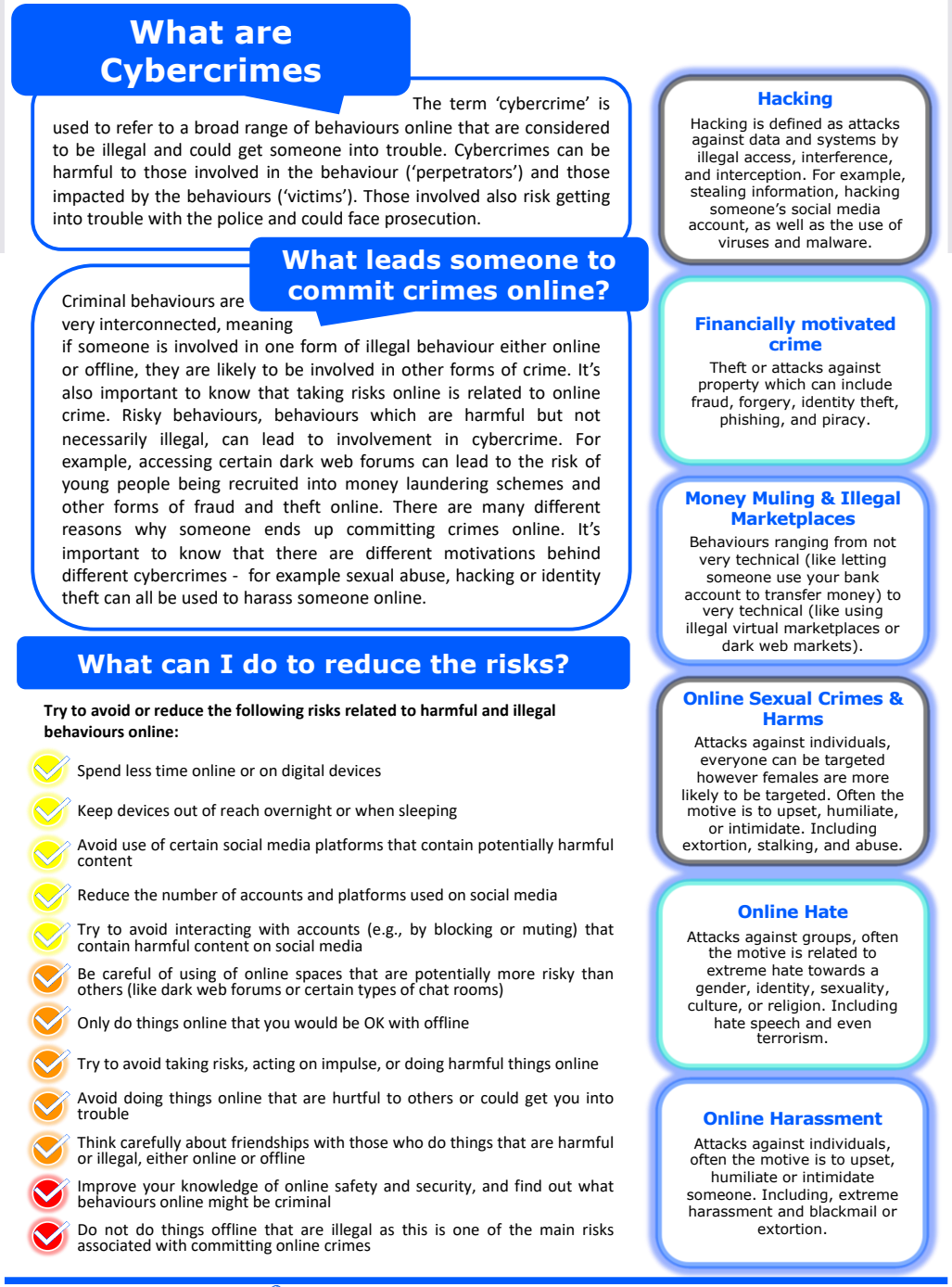
-X5 short educational films for children about the MV and how to keep yourself and others safe. Co-developed with children -

https://www.youtube.com/watch?v=ESy8E5Szs90

Avoiding Cybercrime- Safer Internet Day 2023

Evidence-based educational materials

1) **A "What are cybercrimes?" Poster**
   - To educate young people and adults on what types of online behaviours are risky, harmful, or criminal
2) **A "Crossing the line into Cybercrime" Youth Quiz and Score Sheet**
   - For ages 12+ informed by our research
   - to educate young people about potential online risks and what measures can be taken to reduce and avoid behaviours that are risky, harmful, and associated with online crime
3) **"Pathways into Cybercrime" Resource for parents, caregivers, and educators**
   - Complimentary information as in the quiz but for adults



Child Online Harms Think Tank

CHILD ONLINE HARMS POLICY THINK TANK

An independent, academic initiative dedicated to informing policy on child online harms by leveraging a peer reviewed, research evidence-based approach.

Aims:

1. **To inform UK (and international) policy on child online harms using a research evidence-based approac**h
2. **Engage directly with policy makers to identify key evidence from research to inform policy issues**
3. **To seek funding to undertake and fund short, timely research projects in key areas where gaps exist**
4. **Identify emergent risks and consider policy implications**

Focus

CHILD ONLINE HARMS POLICY THINK TANK

Areas of initial focus:

1. Risks in Virtual Reality/ the Metaverse: Safeguarding Children in Immersive Spaces
2. Youth Online Offending: Understanding Cybercrime Pathways*
3. Understanding Risk and Harm in the context of Early Years
4. Confronting Toxic Masculinity Among Young Boys Online

* Davidson J & Farr, R (2025 forthcoming) '*Youth Pathways into and out of Cybercrime*' Routledge

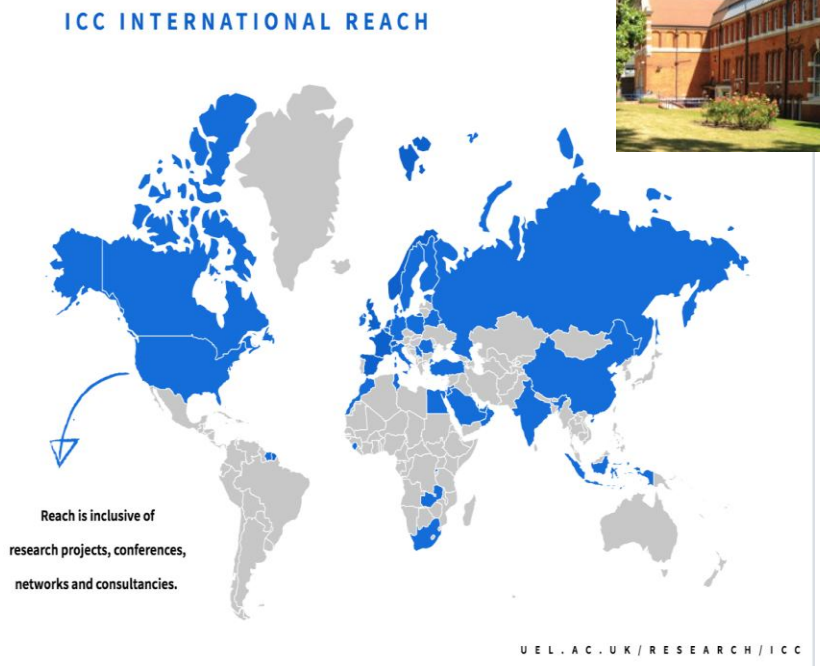
UEL Institute for Connected Communities

Thanks for listening!

j.Davidson@uel.ac.uk

Twitter X - @juliadavidson13

See our research here:
https://uel.ac.uk/our-research/institute-connected-communities-icc



University of East London

THE INSTITUTE FOR CONNECTED COMMUNITIES