TRAINING OF TRAINERS MODULE FOR FRONTLINE PROFESSIONALS ON SAFEGUARDING CHILDREN FROM ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

End Online Child Sexual
Exploitation and Abuse @Europe Plus

Building a Europe
for and with children

www.coe.int/children

Safe Online

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

TRAINING OF TRAINERS MODULE FOR FRONTLINE PROFESSIONALS ON SAFEGUARDING CHILDREN FROM ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

End Online Child Sexual Exploitation and Abuse @Europe Plus

Author:
David Wright

Peer review:
Hélène Paillard

Council of Europe

The opinions expressed in this book may not reflect the views of the Council of Europe or those of Safe Online.

The Council of Europe gratefully acknowledges the financial support provided for this project by Safe Online.

Safe Online is the only global investment vehicle dedicated to keeping children safe in the digital world. Through investing in innovation and bringing key actors together, Safe Online helps shape a digital world that is safe and empowering for all children and young people, everywhere. Learn more at https://safeonline.global/.

All other correspondence concerning this document should be addressed to the Directorate General of Democracy and Human Dignity,
Council of Europe, F-67075 Strasbourg Cedex
E-mail: children@coe.int

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Cover photo: © Shutterstock

Cover design and layout: Tipografia „Foxtrot" SRL,
1 Florilor St., Chişinău Municipality, Republic of Moldova

Table of Contents

INSTRUCTIONS 5
COURSE OBJECTIVE 7
COURSE STRUCTURE 9
COURSE SYLLABUS / AGENDA 11
COURSE CONTENT 15
1. Presentation 15
2. Introductions 18
3. Changing Technologies 19
4. What is Online Safety? 22
5. Specific Online Safety/Child Protection Issues 24
5.1 Online Child Sexual Exploitation and Abuse 38
6. Research Evidence 55
7. Scenarios 56
8. Future Technologies 58
9. Online Safety strategies for educators, social workers and doctors 66
10. Online Safety Strategies for Parents 74
11. Existing Practice 83
12. Online Safety Resources 84
13. National Framework 85
14. Summary 86

Instructions

This handbook serves as a comprehensive training resource for trainers of frontline professionals working with children, particularly those training teachers, doctors, and social workers. Its purpose is to equip trainers with the essential skills, knowledge, and tools needed to effectively protect children from online risks, including online child sexual exploitation and abuse, and to enable them to transfer this knowledge to professionals working directly with children.

The content is intentionally general in nature, designed to be reusable and adaptable across various national contexts. Trainers are encouraged to supplement this handbook with more specific, locally relevant information tailored to their national or regional settings. To support this, designated sections have been included throughout the handbook. These sections, *highlighted in grey and formatted in italic text*, provide space for trainers to incorporate context-specific content.

Course Objective

The primary objective of the Online Safety Train the Trainer Programme is to empower a select group of trainers in Georgia, Republic of Moldova, and Montenegro with the necessary skills, knowledge, and resources to effectively safeguard children from online risks. These trainers will, in turn, cascade the training to other professionals within their countries, creating a ripple effect that amplifies the reach and impact of the programme.

Specific Objectives

1. **Enhance Awareness and Understanding of Online Safety**: Participants will develop a deep understanding of the various risks associated with children's use of technology, with a focus on online child sexual exploitation and abuse. This includes not only understanding the different types of online threats but also recognising the psychological and social factors that exacerbate these risks.
2. **Equip Trainers with Practical Skills**: The programme is designed to provide trainers with practical skills to identify, respond to, and mitigate online safety risks. This includes learning about the latest tools, strategies, and technologies that can be used to protect children online.
3. **Foster Critical Thinking and Problem-Solving**: Through scenario-based exercises and discussions, participants will enhance their critical thinking and problem-solving abilities. They will learn to apply theoretical knowledge to practical situations, making them more effective in real-world contexts.
4. **Promote Best Practices and Policy Development**: Participants will explore and share best practices in online safety, helping to establish a framework of effective strategies and policies that can be implemented within their own organisations and communities.
5. **Build Capacity for Continuous Learning and Adaptation**: The digital landscape is constantly evolving, and so too are the risks associated with it. The programme aims to instil a mindset of continuous learning and adaptation, ensuring that trainers remain up to date with the latest developments in online safety.
6. **Facilitate Collaborative Learning and Networking**: By bringing together professionals from different sectors and countries, the programme fosters a collaborative learning environment. Participants will have the opportunity to network, share experiences, and learn from each other, building a community of practice that extends beyond the training itself.
7. **Empower Trainers to Cascade Knowledge**: Ultimately, the programme aims to equip trainers with the confidence and capability to cascade their knowledge and skills to other professionals in their respective countries. This multiplier effect ensures a broader and more sustained impact, reaching a larger audience and creating safer online environments for children.

Outcomes

By the end of the two-day training, participants will:

- Have a comprehensive understanding of the current online safety landscape, including emerging technologies and associated risks.

- Be proficient in identifying and addressing specific online safety issues related to online child sexual exploitation and abuse but also have a broader awareness of related issues such as cyberbullying, misinformation, device security, and persuasive design in technology.
- Possess practical strategies and tools to implement effective online safety measures within their organisations and communities.
- Be able to engage and educate parents on managing their children's digital lives, promoting healthy technology use, and safeguarding privacy.
- Have established connections with other professionals, creating a support network for ongoing collaboration and knowledge sharing.
- Be prepared to deliver further training to colleagues and other stakeholders, thereby extending the reach and impact of the programme.

The Online Safety Train the Trainer Programme is a comprehensive initiative aimed at creating a safer digital environment for children by empowering those on the front lines of child protection.

Course Structure

The two-day programme is structured to build understanding, explore specific online safety issues, and provide practical strategies for application.

Day 1: Landscape and Challenges

The training begins with introductions, setting a collaborative tone and fostering a sense of community among participants. This is followed by a session on Changing Technologies, where trainers learn about the rapid evolution of technology and its implications for children, including both opportunities and risks.

Next, a comprehensive discussion on What is Online Safety? provides participants with an understanding of the various risks associated with children's use of technology, focusing on Content, Contact, Conduct, and Contract. This foundational knowledge is crucial for identifying and mitigating risks.

After a break, the focus shifts to Specific Online Safety/Child Protection Issues. Participants explore broader aspects that relate to online child sexual exploitation and abuse and how they might be connected and include the psychological impact of persuasive design in technology, challenges in device security, misinformation and disinformation, online bullying, harmful content, and the influence of technology and peer pressure on children's well-being. The session then focuses on online child sexual exploitation and abuse, including an overview of specific threats and harms.

A review of national and international academic research on online safety provides an evidence base that supports the strategies and practices discussed. Practical exercises using scenarios follow, helping participants apply their learning to real-world situations.

The day concludes with a forward-looking session on Future Technologies, where participants learn to anticipate and prepare for future challenges in safeguarding children.

Day 2: Strategies and Management

The second day begins with a review of the key points covered on the first day, reinforcing learning. The first major session focuses on Online Safety Strategies for educators, social workers and doctors, exploring organisational strategies to create and maintain a safe online environment for children.

Following this, a session on Online Safety Strategies for Parents equips participants with practical tools and resources to help parents manage their children's digital lives effectively. Topics include managing screentime, privacy settings, modelling healthy technology use, and handling peer pressure.

Participants then share their current practices in the Existing Online Safety Practice session, learning from each other's experiences and identifying effective strategies. An important element is the presentation of specific national prevention, reporting and referral mechanisms.

Next, participants are guided through a variety of Effective Online Safety Resources, equipping them with valuable tools to support their ongoing efforts. The training concludes with a summary session, reviewing all content covered and addressing any remaining questions.

Throughout the contributions will be benefit from a combination of broad aspects from international experts, supplemented by local context provided by national experts.

By the end of the programme, participants will have a comprehensive understanding of online safety and the confidence to cascade this knowledge effectively within their respective countries. This structured approach ensures that trainers are well-prepared to make a significant impact in safeguarding children in the digital world.

Course Syllabus / Agenda

DAY 1 – LANDSCAPE AND CHALLENGES

Introductions (30 minutes)

To introduce the course and its objectives, delegates and trainers

Changing Technologies (60 minutes)

Technology changes at an astonishing rate; what are the emerging technologies and the opportunities these afford to children

What is Online Safety? (60 minutes)

General discussion covering the array of risks that technology presents to children, specifically the 4 C's (Content, Contact, Conduct and Contract)

Lunch break

Specific Online Safety / Child Protection Issues (120 minutes)

An opportunity to explore and discuss broader online safety risks in more depth and how these may relate to online child sexual exploitation and abuse, specifically:

- **Health and Wellbeing**: Technology and services are designed to persuade and compel users to keep using and returning. The session will explore examples of persuasive design, touching on underlying psychology, that not only affect children, but also parents, potentially drawing their attention away from their children.
- **Cyber Security**: Device security is increasingly challenging with organised crime.
- **Misinformation and Disinformation**: GenAI is revolutionising technology and content creation, not all of which is accurate.
- **Bullying**: Exploration of online bullying and the impact that this can have.
- **Harmful Content**: A review of vulnerability – Those at most risk online, are those at most risk in the physical world.
- **Influence**: A review of the influence that technology (influencers) and surroundings (peer, sibling) have on children and how this impacts (body image, FOMO, etc.).

A focused session on **Online Child Sexual Exploitation and Abuse**, looking at:

- Harmful Sexual Behaviour online,
- Child sexual Abuse Material, including synthetic CSAM,

- Financial extortion,
- Child exploitation online,
- OCSEA Threat Assessment.

Research Evidence (30 minutes)

Literary review of published academic research (national and international) into online safety.

Scenarios (60 minutes)

Using scenarios, an exercise to discuss the implications on children and how to respond.

Future Technologies (60 minutes)

Looking forward, a look at emerging technology, particularly GenerativeAI and the potential risks to children – what will delegates need to consider into the future to protect them?

DAY 2 – STRATEGIES AND MANAGEMENT

Review of Day 1 (30 minutes)

A brief summary, highlighting the aspects covered during day 1

Online Safety strategies for Educators, social workers and doctors (90 minutes)

A detailed discussion of what strategies, policies and tools an organisation could have in place to effectively protect children online, specifically:

- Ownership
- Reporting
- Policy
- Staff Development
- Children's education
- Securing Technology
- Evaluation

Online Safety strategies for Parents (90 minutes)

An exploration of strategies, tools and resources available for parents to manage their families use of technology and creating the right environment, specifically:

- Understanding access and services – identifying the devices their family has and the services used by their children to determine the extent of online access.
- Conversation starters – suggestions to initiate discussions about staying safe online and a healthy digital balance.
- Family Sharing Tools and managing the challenge of screentime – a resume of the availability of tools available to parents to manage and limit their children's use of both devices and services. Extending to examples to manage screentime, specifically overnight and at mealtimes.
- Managing access – a discussion leading on from parental tools to look at physical measures to managing access, including when to give the first mobile phone, liaising with other parents to combat peer pressure and SMART family agreements.

- Managing privacy settings – a summary of the privacy settings available across the most popular social media services and how to access these.
- Digital Role Model (as a parent) – awareness of parents' use of technology and the importance of modelling healthy technology use.
- Managing influence – how to initiate healthy discussions with children around understanding the influence of online content (eg on body image) and also how to manage peer pressure.
- Minimum age requirements – a summary of the most popular online services and their associated minimum age requirements.

Lunch break

Existing Online Safety Practice (60 minutes)

The opportunity to consider and share amongst delegates your existing online safety measures and practice. The session will establish examples of good practice.

Effective Online Safety Resources (30 minutes)

Signposting effective online safety resources

National Framework (60 minutes)

An overview of the specific national prevention, reporting and referral mechanisms, alongside existing protocols for each category of professionals in cases of violence against children

Summary (30 minutes)

A review of all content covered and affording delegates the opportunity to ask clarification and consolidation questions

Course Content

1. PRESENTATION

Slide 1

The primary objective of the Online Safety Train the Trainer Programme is to empower a select group of trainers in Georgia, Republic of Moldova, and Montenegro with the necessary skills, knowledge, and resources to effectively safeguard children from online risks. These trainers will, in turn, cascade the training to other professionals within their countries, creating a ripple effect that amplifies the reach and impact of the programme.

Specific Objectives

Enhance Awareness and Understanding of Online Safety: Participants will develop a deep understanding of the various risks associated with children's use of technology, with a focus on online child sexual exploitation and abuse. This includes not only understanding the different types of online threats but also recognising the psychological and social factors that exacerbate these risks.

Equip Trainers with Practical Skills: The programme is designed to provide trainers with practical skills to identify, respond to, and mitigate online safety risks. This includes learning about the latest tools, strategies, and technologies that can be used to protect children online.

Foster Critical Thinking and Problem-Solving: Through scenario-based exercises and discussions, participants will enhance their critical thinking and problem-solving abilities effective in real-world contexts.

Promote Best Practices and Policy Development: Participants will explore and share best practices in online safety, helping to establish a framework of effective strategies and policies that can be implemented within their own organisations and communities.

Build Capacity for Continuous Learning and Adaptation: The digital landscape is constantly evolving, and so too are the risks associated with it. The programme aims to instil a mindset of continuous learning and adaptation, ensuring that trainers remain up to date with the latest developments in online safety.

Facilitate Collaborative Learning and Networking: By bringing together professionals from different sectors and countries, the programme fosters a collaborative learning environment. Participants will have the opportunity to network, share experiences, and learn from each other, building a community of practice that extends beyond the training itself.

Empower Trainers to Cascade Knowledge: Ultimately, the programme aims to equip trainers with the confidence and capability to cascade their knowledge and skills to other professionals in their respective countries. This multiplier effect ensures a broader and more sustained impact, reaching a larger audience and creating safer online environments for children.

Outcomes

By the end of the two-day training, participants will:

- Have a comprehensive understanding of the current online safety landscape, including emerging technologies and associated risks.

- Be proficient in identifying and addressing specific online safety issues related to online child sexual exploitation and abuse but also have a broader awareness of related issues such as cyberbullying, misinformation, device security, and persuasive design in technology.
- Possess practical strategies and tools to implement effective online safety measures within their organisations and communities.
- Be able to engage and educate parents on managing their children's digital lives, promoting healthy technology use, and safeguarding privacy.
- Have established connections with other professionals, creating a support network for ongoing collaboration and knowledge sharing.
- Be prepared to deliver further training to colleagues and other stakeholders, thereby extending the reach and impact of the programme.

Slide 2 – Content (Day 1)

The course will cover the following modules:

1. **Introductions**: Moment to introduce participants to the training and trainers
2. **Changing technologies**: Technology changes at an astonishing rate; what are the emerging technologies and the opportunities these afford to children.
3. **What is Online Safety?** General discussion covering the array of risks that technology presents to children, specifically the 4 C's (Content, Contact, Conduct and Contract).
4. **Specific Online Safety/Child Protection Issues**: An opportunity to explore and discuss broader online safety risks in more depth and how these may relate to **online child sexual exploitation and abuse**, specifically:
    - Health and Wellbeing
    - Cyber Security
    - Misinformation and Disinformation
    - Bullying
    - Harmful Content
    - Influence

    A focused session on Online Child Sexual Exploitation and Abuse, looking at:

    - Harmful Sexual Behaviour online
    - Child sexual Abuse Material, including synthetic CSAM
    - Financial extortion
    - Child exploitation online
    - OCSEA Threat Assessment
5. **Research Evidence**: Literary review of published academic research (national and international) into online safety.
6. **Scenarios**: Using scenarios, an exercise to discuss the implications on children and how to respond.
7. **Future Technologies**: Looking forward, a look at emerging technology, particularly GenerativeAI and the potential risks to children – what will delegates need to consider into the future to protect them?

End of Day 1

Slide 3 – Content (Day 2)

At the start of Day 2 we will first Recap Day 1.

1. **Online Safety strategies for Educators, social workers and doctors**: A detailed discussion of what strategies, policies and tools an organisation could have in place to effectively protect children online, specifically:
    - Ownership

- Reporting
- Policy
- Staff Development
- Children's education
- Securing Technology
- Evaluation

2. **Online Safety strategies for Parents**: An exploration of strategies, tools and resources available for parents to manage their families use of technology and creating the right environment, specifically:
   - Understanding access and services – identifying the devices their family has and the services used by their children to determine the extent of online access.
   - Conversation starters – suggestions to initiate discussions about staying safe online and a healthy digital balance.
   - Family Sharing Tools and managing the challenge of screentime – a resume of the availability of tools available to parents to manage and limit their children's use of both devices and services. Extending to examples to manage screentime, specifically overnight and at mealtimes.
   - Managing access – a discussion leading on from parental tools to look at physical measures to managing access, including when to give the first mobile phone, liaising with other parents to combat peer pressure and SMART family agreements.
   - Managing privacy settings – a summary of the privacy settings available across the most popular social media services and how to access these.
   - Digital Role Model (as a parent) – awareness of parents' use of technology and the importance of modelling healthy technology use.
   - Managing influence – how to initiate healthy discussions with children around understanding the influence of online content (e.g. on body image) and also how to manage peer pressure.

   Minimum age requirements – a summary of the most popular online services and their associated minimum age requirements.
3. **Existing Online Safety Practice**: The opportunity to consider and share amongst participants your existing online safety measures and practice. The session will establish examples of good practice.
4. **National Framework**: An overview of the specific national prevention, reporting and referral mechanisms, alongside existing protocols for each category of professionals in cases of violence against children.
5. **Online Safety Resources**: Signposting effective online safety resources.
6. **Summary**: A review of all content covered and affording participants the opportunity to ask clarification and consolidation questions.

2. INTRODUCTIONS

Slide 4

To go round the room and everyone to introduce themselves and their organisation.

Slide 5

Presentation of the national trainer.

Slide 6

Presentation of the national trainer's organisation/centre.

Slide 7 – Train the Trainer notes

(O)CSEA is a sensitive topic, and remember the importance of creating a friendly, informal atmosphere so that people feel comfortable talking about it.

Trainers should agree beforehand on a procedure in the event that a trainee comes forward as a CSEA victim.

3. CHANGING TECHNOLOGIES

Slide 8

Changing Technologies Section – Technology changes at an astonishing rate; what are the emerging technologies and the opportunities these afford to children.

Slide 9 – The Extent of Technology in Homes

Introduction: In this slide, we'll explore the growing presence of connected technologies in our homes. Traditionally, we consider laptops, tablets, and mobile phones, but many homes now include a wide range of smart devices. This discussion aims to encourage participants to think about the extent of technology in their homes and its implications for privacy and security.

Slide Overview:

Objective: Highlight the variety of connected devices in modern homes and discuss their impact on family life and security.

Key Points:

- **Traditional Devices:**
  - **Laptops, Tablets, and Mobile Phones:** Discuss the widespread use of these traditional devices in everyday life for communication, work, and entertainment.
- **Connected Kitchen:**
  - **Smart Appliances:** Mention smart fridges that can track inventory and suggest recipes, smart ovens that can be controlled remotely, and smart bulbs that adjust lighting.
  - **Central Heating:** Highlight smart thermostats that learn user preferences and can be controlled via smartphone apps.
- **Living Room Technology:**
  - **Smart TVs:** Discuss how smart TVs offer streaming services, internet browsing, and integration with other smart home devices.
  - **Smart Speakers:** Explain the role of smart speakers like Amazon Echo and Google Home in controlling other devices, playing music, and answering queries.
- **Children's Rooms:**
  - **Gaming Consoles:** Mention popular gaming consoles like PlayStation and Xbox that offer not just gaming but also streaming services and online interaction.
  - **Educational Devices:** Highlight smart toys and devices used for educational purposes that connect to the internet for content updates and interaction.
- **Home Office:**
  - **Computers and Printers:** Discuss the essential role of computers and printers in a home office setup.

  - **Networking Equipment:** Mention routers and modems that are crucial for internet connectivity and often include smart features.
- **The Cloud:**
  - **Data Storage:** Explain how many households use cloud services for storing documents, photos, and other important files. Highlight the convenience and potential privacy concerns of cloud storage.

Action Steps:

- **Interactive Exercise:** Ask delegates to list all the connected devices in their homes room by room. Potentially provide a template or worksheet for this activity.
- **Discussion Questions:**
  - "What are some of the benefits and challenges associated with having multiple connected devices in the home?"
  - "How do you ensure the security of these devices?"
- **Resource Sharing:** Provide links to resources on securing smart home devices and managing privacy settings.

Discussion:

- **Personal Experiences:** Invite delegates to share their experiences with smart home devices. What benefits have they seen? What challenges have they faced?
- **Security Measures:** Discuss common security measures such as changing default passwords, keeping software updated, and using two-factor authentication.

Conclusion: The growing number of connected devices in our homes offers many conveniences but also poses privacy and security challenges. By understanding the extent of technology in our homes, we can take steps to protect our families and personal information.

Slide 10 – National Data on Children's Use of Technology

Introduction: In this section, we'll examine the national data on children's use and experience of technology. The example provided is from Ofcom, which offers valuable insights into the digital habits and safety concerns of children in the UK. This data serves as a model for understanding similar trends in other regions and can be complemented or replaced with more specific national evidence where available.

Slide Overview:

- **Objective:** Highlight the importance of national data in understanding children's technology use and experiences, and encourage the use of local data where available.

Key Points:

- **Purpose of National Data:**
  - **Understanding Trends:** National data helps identify trends in how children interact with technology, including usage patterns and popular platforms.
  - **Policy Making:** This data informs policymakers, educators, and parents, aiding in the development of effective strategies for digital safety and education.
  - **Comparative Analysis:** Allows for comparison between different regions, helping to identify unique challenges and best practices.
- **Example: Ofcom Data (UK):**
  - **Usage Statistics:** Discuss the percentage of children using various types of devices and the frequency of their usage.
  - **Platform Popularity:** Highlight which platforms (e.g., social media, gaming) are most popular among children.
  - **Safety Concerns:** Share statistics on issues like cyberbullying, privacy concerns, and exposure to inappropriate content.

- **Implications of the Data:**
  - **Parental Awareness:** Emphasise the need for parents to be aware of their children's digital activities and the platforms they use.
  - **Educational Initiatives:** Highlight how schools can use this data to integrate digital literacy and safety into the curriculum.
  - **Policy Development:** Discuss how policymakers can leverage this data to create safer online environments for children.
- **Encouragement of Local Data Use:**
  - **Relevance:** Stress the importance of using local data to ensure relevance and applicability to the audience's specific context.
  - **Accessibility:** Provide tips on where to find local data, such as government reports, academic studies, and surveys from local organisations.
  - **Adaptability:** Suggest ways to adapt the findings from national data to local settings, considering cultural and regional differences.

Action Steps:

- **Interactive Exercise:** Ask participants to share any national data or reports they are aware of from their own countries. Encourage discussion on how this data can be utilised in their professional practices.
- **Discussion Questions:**
  - "What are some of the key findings from the national data on children's technology use in your country?"
  - "How can we apply these findings to improve digital safety and education in our local communities?"
- **Resource Sharing:** Provide links to relevant national reports and databases where delegates can find additional information.

Discussion:

- **Personal Experiences:** Invite participants to share their experiences with national data. How has it helped them in their roles? What gaps do they see in the available data?
- **Data Utilisation:** Discuss practical ways to use this data to inform teaching practices, parental guidance, and policymaking.

Conclusion: National data on children's use of technology is crucial for understanding trends, identifying safety concerns, and informing effective policies and practices. By leveraging this data, we can better support children's safe and responsible use of digital technologies.

Slide 11 – National Landscape evidence

[Placeholder for the national trainer to add relevant information.]

4. WHAT IS ONLINE SAFETY?

Slide 12 – Online Safety Section

General discussion covering the array of risks that technology presents to children, specifically the 4 C's (Content, Contact, Conduct and Contract).

Slide 13 – Discussion about what is online safety

Encourage participants to offer their thoughts about what they think Online Safety is – what are the issues that they perceive and experience.

Slide 14 – Online Risks and Threats Facing Children

Introduction

On this slide, we are exploring the categorisation of online risks and threats facing children. Professor Sonia Livingstone's '4 Cs' framework[1] is an effective model for understanding these complex and varied dangers.

Content Slide Breakdown

- **Overview of the '4 Cs'**
  - The '4 Cs' stand for Content, Contact, Conduct, and Contract. These categories encompass the range of risks children face online. Each category highlights different dimensions of potential harm.
- **Content Risks**
  - **Description**: Content risks involve exposure to potentially harmful material.
  - **Examples**: Violent, gory, graphic, racist, hateful, or extremist information, as well as harmful or illegal pornography, sexualisation of culture, and oppressive body image norms.
  - **Impact**: These can negatively affect a child's mental health, development, and worldview.
- **Contact Risks**
  - **Description:** Contact risks refer to harmful interactions with adults online.
  - **Examples:** Harassment, stalking, hateful behaviour, unwanted or excessive surveillance, sexual harassment, grooming, sextortion, and the sharing of, or requesting for child sexual abuse material.
  - **Impact:** Such interactions can lead to psychological and physical danger, manipulation, and exploitation.
- **Conduct Risks**
  - **Description:** Conduct risks are related to how children behave online and how these behaviours can put them at risk.

[1] 4 Cs of online risk: Short report & blog on updating the typology of online risks to include content, contact, conduct, contract risks – CO:RE Knowledge Base (core-evidence.eu).

  - **Examples:** Bullying, hateful or hostile communication, peer activity like trolling, exclusion, shaming, and participating in risky challenges. Requests for self-generated sexual content, sexual harassment, and sextortion.
  - **Impact:** This can result in retaliation, loss of privacy, or physical and psychological danger.
- **Contract Risks**
  - **Description:** Contract risks involve exploitation through commercial activities.
  - **Examples:** Identity theft, fraud, phishing, scams, hacking, blackmail, security risks, selling/buying CSAM, livestreaming, and trafficking for sexual exploitation.
  - **Impact:** Children can suffer financial loss, unauthorised charges, and compromised personal information. As an additional note, child trafficking may result in [severe] traumas, PTSD, stigmatisation, discrimination, isolation, reproductive health issues, etc.

Cross-Cutting Issues: Additionally, these risks have cross-cutting issues including privacy violations, physical and mental health risks, and inequalities and discrimination. These underline the pervasive nature of online risks and emphasise the need for comprehensive protective measures.

Discussion Points – Questions to Engage the Audience:

- How do you see these risks manifesting in your professional experience?
- What strategies have you found effective in mitigating these risks for children?

Closing Remarks

Understanding the '4 Cs' framework helps us to better protect children in the digital age. It highlights the importance of vigilance and proactive measures to ensure their safety and well-being online.

5. SPECIFIC ONLINE SAFETY/CHILD PROTECTION ISSUES

Slide 15

An opportunity to explore and discuss broader online safety risks in more depth and how these may relate to online child sexual exploitation and abuse – What are the specific child protection issues?

Slide 16 – General Issues Affecting Children's Online Safety

Slide Overview:

- **Content:** Introduction to six key issues: Health and Wellbeing, Cyber Security, Misinformation and Disinformation, Bullying, Harmful Content, and Influence.

Key Points to Cover:

- **Introduction to General Issues:**
  - Importance of understanding various online safety issues impacting children.
  - Interconnected nature of these issues requires a comprehensive approach.
- **Health and Wellbeing:** Technology and services are designed to persuade and compel users to keep using and returning. The session will explore examples of persuasive design, touching on underlying psychology, that not only affect children, but also parents, potentially drawing their attention away from their children.
- **Cyber Security:** Device security is increasingly challenging with organised crime.
- **Misinformation and Disinformation:** Generative AI is revolutionising technology and content creation, not all of which is accurate.
- **Bullying:** Exploration of online bullying and the impact that this can have.
- **Harmful Content:** A review of vulnerability – Those at most risk online, are those at most risk in the physical world.
- **Influence:** A review of the influence that technology (influencers) and surroundings (peer, sibling) have on children and how this impacts (body image, FOMO (fear of missing out), etc).

We will then have a focused Session on Online Child Sexual Exploitation and Abuse:

- Importance of understanding and addressing online child sexual exploitation and abuse (OCSEA).
- Key topics to be covered in the next session:
  - Harmful Sexual Behaviour Online
  - Child Sexual Abuse Material, including synthetic CSAM
  - Financial Extortion
  - Child Sexual Exploitation Online
  - OCSEA Threat Assessment

Slide 17 – Online Influence

Slide Overview:

- **Content:** Exploration of how children are influenced online using examples and case studies.

Key Points to Cover:

- **Introduction to Online Influence:**
  - Significance of understanding how children are influenced in the digital world.
  - Various sources of influence including social media, influencers, peers, and technology itself.
- **Mechanisms of Influence:**
  - Algorithms and personalised content that target children's interests and behaviours.
  - The role of social media influencers in shaping children's opinions, behaviours, and self-image.
  - Peer influence through social networks and online interactions.
- **Types of Influence:**
  - Positive influence: educational content, supportive communities.
  - Negative influence: body image issues, fear of missing out (FOMO), peer pressure.
- **Discussion Points:**
  - How parents and educators can help children navigate online influence.
  - Strategies to encourage critical thinking and media literacy among children.
  - The importance of monitoring and setting boundaries for online activity.
- **Engagement Tips:**
  - Encourage participants to share their observations or concerns about children's online behaviour.
  - Use real-life examples and case studies to illustrate the points.
  - Allocate time for questions and discussions to deepen understanding.

Slide 18

Play Video clip – This video discloses that often great care is taken to manicure how you appear online and is not always true or reflective of real life.

Body image as an example.

Body Image Issues Online:

- **Exposure to Idealised Images:** Social media platforms often showcase edited, filtered, and idealised images of beauty and body standards, which can create unrealistic expectations.
- **Comparison Culture:** Constant exposure to these images leads to comparison, making individuals, especially young people, feel inadequate or dissatisfied with their own bodies.
- **Peer Pressure:** Online interactions can include comments and likes that reinforce the importance of appearance, increasing pressure to conform to these ideals.
- **Cyberbullying:** Negative comments and body shaming can exacerbate body image issues and contribute to low self-esteem and mental health problems.

Effects of Online Influence:

- **Mental Health:** Negative body image influenced by online content can lead to depression, anxiety, eating disorders, and other mental health issues.
- **Behavioural Changes:** Individuals might engage in unhealthy behaviours, such as extreme dieting or excessive exercise, to achieve perceived ideal body standards.
- **Self-Esteem:** Frequent comparisons and negative feedback can significantly lower self-esteem and self-worth.

Overall Impact

Online influence profoundly affects body image by promoting unrealistic standards, fostering a culture of comparison, and sometimes leading to harmful mental health and behavioural outcomes.

Slide 19 – Health and Wellbeing

Slide 20 – Time Spent Online

Questions for discussion:

- How much time do children spend online?
- How much time do adults spend online?
- Does the group spend too much or too little time online?

Slide 21 – Mental Health and Wellbeing – Persuasive Design

Slide Overview:

- **Content:** Examination of how persuasive design in technology impacts mental health and wellbeing, with examples and interactive questions.

Key Points to Cover:

- **Introduction to Persuasive Design:**
  - Definition: Persuasive design involves using psychological principles to influence user behaviour.
  - Purpose: Designed to monopolise users' time and keep them engaged with devices and services.
- **Interactive Questions to Engage Audience:**
  - **Question:** "What was the very first thing you did this morning when you woke up?"
    - Likely answer: Checked news, messages, or social media feed on a mobile device.
  - **Question:** "When was the last time you checked your phone?"
    - Emphasise the frequency and automatic nature of this behaviour.
- **Explanation of Persuasive Design Techniques:**
  - **Refresh Mechanism:**
    - Analogy: Compared to gambling and a slot machine.
    - Action: Pull down to refresh inbox or social media stream, similar to pulling a slot machine handle.
    - Impact: Creates anticipation and compels users to keep checking for new updates.
  - **Snapstreaks:**
    - Definition: A feature in Snapchat where users send snaps back and forth consecutively to maintain a streak.
    - Impact: Encourages daily engagement and regular interaction to avoid breaking the streak.
  - **Three Dots (Typing Indicators):**
    - Description: The pulsating dots indicating someone is replying to a message.
    - Purpose: Keeps users in the messaging app, waiting for the response.
    - Effectiveness: Increases time spent in the app as users wait for incoming messages.
- **Impact on Mental Health and Wellbeing:**
  - Increased screen time can lead to:
    - Anxiety and stress.

        - Disrupted sleep patterns.
        - Reduced face-to-face social interactions.
    - Continuous engagement with devices can draw attention away from real-life interactions and responsibilities.
- **Discussion Points:**
    - How can users become more aware of these design techniques?
    - What strategies can be employed to reduce the negative impact of persuasive design?
    - Role of parents and educators in helping children manage screen time and develop healthy digital habits.

Engagement Tips:

- Encourage the audience to share their experiences with persuasive design features.
- Use real-life examples and demonstrate using a mobile device.
- Allocate time for questions and reflections to deepen understanding.

Slide 22 – Cyber Security

Slide 23 – Intersect of Cybersecurity, Online Safety, Safeguarding, and Media Literacy

Slide Overview:

- **Content:** Discussion on the interconnectedness of cybersecurity, online safety, safeguarding, and media literacy.

Key Points to Cover:

- **Introduction to Interconnected Concepts:**
    - Explain that cybersecurity, online safety, safeguarding, and media literacy are not isolated concepts; they often overlap and influence each other.
    - Highlight the importance of understanding these intersections to create a holistic approach to digital well-being.
- **Definitions:**
    - **Cybersecurity:** Protection of internet-connected systems, including hardware, software, and data, from cyberattacks.
    - **Online Safety:** Practices and technologies to protect users, particularly children, from online dangers such as cyberbullying, exploitation, and inappropriate content.
    - **Safeguarding:** Measures to protect individuals, especially children and vulnerable adults, from harm, abuse, and exploitation, both online and offline.
    - **Media Literacy:** The ability to access, analyse, evaluate, and create media in various forms, understanding the role of media in society.
- **Examples of Interconnectedness:**
    - **Example 1: Phishing Scams**
        - **Cybersecurity Aspect:** Technical measures to detect and prevent phishing attempts.
        - **Online Safety Aspect:** Educating users on recognising phishing emails and not clicking on suspicious links.
        - **Safeguarding Aspect:** Protecting sensitive information from being exploited by malicious actors.
        - **Media Literacy Aspect:** Understanding how phishing scams are crafted and the motives behind them.
    - **Example 2: Social Media Use**
        - **Cybersecurity Aspect:** Ensuring privacy settings are configured to protect personal data.

        - **Online Safety Aspect:** Being aware of the potential for cyberbullying and online predators.
        - **Safeguarding Aspect:** Monitoring and guiding children's social media interactions to ensure their safety.
        - **Media Literacy Aspect:** Critically evaluating the content encountered on social media and understanding its potential impact.
- **Importance of an Integrated Approach:**
    - Emphasise that addressing these areas in isolation can lead to gaps in protection and education.
    - Integrated approach ensures comprehensive protection and empowers users with knowledge and skills to navigate the digital world safely.
- **Practical Implications:**
    - **For Educators:** Incorporate lessons that cover all these aspects to provide students with a well-rounded understanding of digital safety.
    - **For Parents:** Stay informed and involved in children's online activities, combining technical protections with open conversations about online behaviour.
    - **For Policy Makers:** Develop policies that reflect the interconnected nature of these areas, ensuring cohesive and effective regulations.

Engagement Tips:

- Use real-life scenarios to illustrate how these concepts intersect in everyday digital interactions.
- Encourage audience participation by asking them to share their experiences with online safety and cybersecurity challenges.
- Provide practical tips and resources for integrating these aspects into daily routines.

Slide 24 – Cybersecurity threats to Schools

Slide Overview:

- **Content:** Emphasise that schools and organisations working with children are prime targets for cybersecurity scams. Mention relevant national data on the frequency of data breaches. *[Placeholder for the national trainer to add relevant information.]*

Key Points to Cover:

- **Introduction to Cybersecurity Threats:** Highlight the increasing number of cybersecurity attacks targeting schools and organisations that work with children.
- **Data Breaches in Schools:** Mention that schools are particularly vulnerable to data breaches due to the valuable personal information they hold, such as student records and staff details.
- **National Data Example:**
    - Replace the UK example with relevant national data showing the prevalence of data breaches in schools. *[Placeholder for the national trainer to add relevant information.]*
    - Example statement: "Recent national data indicates that schools are significantly more targeted by cyberattacks compared to other sectors."
- **Reasons for Targeting Schools:** Discuss why schools are attractive targets:
    - They store sensitive personal information.
    - They may have weaker cybersecurity defences.
    - Limited resources for robust cybersecurity measures.
- **Impact of Cybersecurity Breaches:** Explain the consequences of data breaches in schools:
    - Disruption to educational activities.
    - Financial costs for remediation.

  - Loss of trust from parents, students, and staff.
  - Potential for identity theft and exploitation of personal information.
- **Importance of Cybersecurity Measures:**
  - Stress the need for strong cybersecurity practices in educational institutions.
  - Mention the importance of training staff and students in recognising and responding to cyber threats.

Engagement Tips:

- Use a simple graphic or chart to illustrate the increase in data breaches targeting schools.
- Encourage discussion by asking the audience if they are aware of any local incidents or measures taken by schools to enhance cybersecurity.

Slide 25 – How Threats Manifest Themselves in Schools

- **Introduction:** This slide highlights how cybersecurity threats are manifesting in schools, using data from the UK as an example. *[Placeholder for the national trainer to add relevant information.]* Schools and organisations working with children are increasingly targeted by cyber threats.
- **Key Points:**
  - **Phishing Attacks:** A significant majority of schools have identified phishing attacks as a prevalent threat.
  - **Impersonation:** Many schools have reported incidents where cybercriminals impersonate their organisations to trick individuals into divulging sensitive information.
  - **Malware:** The presence of viruses, spyware, and other malware has been reported, posing risks to the school's data and network security.
  - **Unauthorised Access by Students:** Incidents of students gaining unauthorised access to files or networks are also noteworthy.
  - **Account Hacking:** Attempts to hack online bank accounts and other critical systems have been identified.
  - **Ransomware Attacks:** Ransomware attacks, where data is encrypted and held hostage for a ransom, are also a concern for educational institutions.
- **Conclusion:** These examples underscore the importance of robust cybersecurity measures in schools and organisations working with children. They need to stay vigilant and proactive in safeguarding against these evolving threats.

***Note:** Replace the UK data with relevant national data to better reflect local threats and scenarios.*

Slide 26 – Misinformation and Disinformation

- **Introduction to Misinformation and Disinformation:**
  - **Misinformation** refers to false or inaccurate information spread without malicious intent. This can occur through rumours, misunderstandings, or unverified information shared widely.
  - **Disinformation** is deliberately created and disseminated with the intent to deceive or mislead. This can involve fabricated stories, manipulated content, and co-ordinated campaigns to influence public opinion or behaviour.
- **Impact on Children:** Misinformation and disinformation can have significant impacts on children, influencing their behaviour, mental health, and perception of reality. Children are particularly vulnerable due to their developing critical thinking skills and higher likelihood of trusting online content.
- **Case Study: The Blue Whale Challenge (2017):**
  - **Background:** The Blue Whale Challenge was a supposed online game that allegedly glorified suicide and included 53 increasingly extreme challenges, culminating in the participant committing suicide.
  - **Reported Impact:** It was claimed that 150 children in the Russian Federation had committed suicide as a result of participating in this challenge.

    - **Reality:** The Blue Whale Challenge was later found to be a fabricated story. Despite numerous warnings and heightened awareness, there was no substantial evidence to support the existence of such a challenge.
    - **Lesson:** This case illustrates how misinformation can create widespread panic and fear, affecting both children and adults. It highlights the importance of verifying information before spreading it.
- **Other Examples: Momo Challenge (2019):**
    - Similar to the Blue Whale Challenge, the Momo Challenge involved reports of a game that encouraged children to perform dangerous tasks, ultimately leading to self-harm or suicide.
    - The challenge involved a creepy character, "Momo," and was widely reported in media, creating fear among parents and children.
    - However, it was also debunked as a hoax, with no verified cases of children being harmed as a result.

Conclusion:

- These examples demonstrate the power and danger of misinformation and disinformation in the digital age. It is crucial to educate children on critical thinking and the importance of verifying information from reliable sources.
- As educators and guardians, we must remain vigilant and proactive in combating the spread of false information to protect the well-being of children.

Slide 27 – Online Bullying

- **Introduction to Online Bullying:**
    - Online bullying, also known as cyberbullying, involves the use of digital platforms such as social media, messaging apps, and gaming communities to harass, threaten, or humiliate individuals.
    - Unlike traditional bullying, online bullying can occur 24/7 and reach a wide audience quickly, exacerbating its impact on victims.
- **Overview of the Issue:**
    - **Prevalence:** Online bullying is a pervasive issue affecting children and adolescents globally. It can take various forms, including spreading rumours, sharing private information, sending threatening messages, and creating harmful content about the victim (including content of sexual nature).
    - **Impact on Victims:** The psychological effects of online bullying can be severe, leading to anxiety, depression, low self-esteem, and even suicidal thoughts. Victims often feel powerless and isolated as the bullying can be relentless and difficult to escape.
- **Evidence and Statistics:**
    - According to **Global Kids Online**[2], a significant number of children experience online bullying. In their study, it was found that:
        - **35%** of children aged 9–17 reported experiencing cyberbullying in the past year.
        - **24%** indicated they had been bullied frequently.
    - Another study by the **Cyberbullying Research Center**[3] reported that about **37%** of students have experienced cyberbullying during their lifetimes, with **30%** experiencing it more than once.
    - **UNICEF**[4] also highlights that children who experience online bullying are more likely to skip school, perform poorly academically, and develop mental health issues (see later the slide on the impact of OCSEA on victims).
- **Case Studies and Real-world Examples:**
    - **Amanda Todd (2012):** Amanda Todd, a 15-year-old from Canada, shared her experience with online bullying through a YouTube video. She had been a victim of cyberbullying and sextortion, which led

[2] International day against violence and bullying | Global Kids Online.
[3] Cyberbullying Data 2019 – Cyberbullying Research Center.
[4] Cyberbullying: What is it and how to stop it | UNICEF.

    to severe depression and ultimately her suicide. Her story brought significant attention to the issue of online bullying and the need for preventive measures.

    - **Megan Meier (2006):** Megan Meier, a 13-year-old from the United States, was harassed through a fake MySpace account created by a neighbour. The relentless bullying led to her suicide, highlighting the dangers of anonymous online harassment.

Interactivity: Discussion – have anyone seen instances of online bullying, also called cyberbullying?

Conclusion:

- The issue of online bullying underscores the need for comprehensive digital literacy education and support systems for victims. Schools, parents, and policymakers must work together to create a safe online environment for children.
- Encouraging open communication, teaching empathy and respect, and implementing strict anti-bullying policies are critical steps in combating online bullying.

Slide 28 – Harmful Online Content

- **Introduction:**
    - Harmful online content can significantly affect children's mental health, behaviour, and overall well-being.
    - This section will step through specific examples to illustrate the different types of harmful content children might encounter online.
- **Examples of Harmful Online Content:**
    - **Violent Content:**
        - Exposure to violent videos, images, and games.
        - Can desensitise children to violence and lead to aggressive behaviour.
    - **Sexual Content:**
        - Access to pornography and explicit material (most US teens have reported having seen pornography at age 13).
        - Can lead to distorted perceptions of sex and relationships, and inappropriate sexual behaviour, or even traumas (depending on the nature of this content)
    - **Hate Speech:**
        - Content promoting racism, xenophobia, and other forms of discrimination.
        - Can instil harmful prejudices and encourage exclusionary behaviour.
    - **Self-Harm and Suicide:**
        - Websites and forums that promote self-harm, eating disorders, and suicide.
        - Examples include the Blue Whale Challenge and other viral trends that glorify self-harm.
    - **Misinformation and Disinformation:**
        - False information regarding health, science, and current events.
        - Can lead to dangerous behaviours and mistrust in credible sources.
- **Discussion Points:**
    - **Impact on Children:**
        - Psychological trauma, anxiety, depression, and other mental health issues.
        - Behavioural changes, including increased aggression or withdrawal.
    - **Role of Parents and Educators:**
        - Importance of monitoring online activity and having open discussions with children (identifying children exposed to harmful content).

        - Teaching critical thinking skills to discern credible information from harmful content.
        - Proposing an appropriate response to children exposed to or engaged with it (psychological, legal, etc.)

Closing Remarks: We will now explore some case studies to exemplify the issues and impact that harmful content has on children.

Slide 29 – Molly Russell Case

- **Introduction:**
    - Tragic case highlighting the impact of harmful online content on youth.
    - Focus on Molly Russell, a 14-year-old girl who took her own life in 2018.
    - Point to note – these case examples are widely covered in the public media. Exercise caution with children's identity.
- **Case Overview:**
    - **Incident Details:**
        - Molly Russell died by suicide in November 2017.
        - The coroner's inquest in 2018 revealed crucial insights into the factors contributing to her death.
    - **Influence of Online Content:**
        - It was discovered that Molly had viewed over 2,000 pieces of depressive, self-harm, or suicidal content on platforms like Instagram and Pinterest.
        - The coroner concluded that this exposure significantly influenced her decision to take her own life.
- **Key Points:**
    - **Platforms Involved:**
        - Instagram and Pinterest were specifically mentioned in the inquest.
        - These platforms have algorithms that can inadvertently promote harmful content by continually suggesting similar material based on previous interactions.
    - **Content Types:**
        - Depressive posts, self-harm imagery, and suicidal ideation content.
        - The sheer volume and nature of the content acted as a negative reinforcement.
- **Discussion Points:**
    - **Impact of Algorithms:**
        - How social media algorithms can create a harmful echo chamber for vulnerable individuals.
        - Importance of regulating and monitoring the content that these algorithms promote.
    - **Role of Social Media Companies:**
        - Discussion on the responsibility of social media platforms to protect their users.
        - Actions taken by these companies since the incident, such as implementing stricter content moderation policies and offering mental health resources.
    - **Preventive Measures:**
        - Importance of parental monitoring and open communication about online activities.
        - Schools and communities need to provide support and education on recognising and dealing with harmful online content.

Closing Remarks:

- The Molly Russell case serves as a stark reminder of the real-life consequences of harmful online content.

- Emphasise the need for collaborative efforts between parents, educators, social media companies, and policymakers to safeguard children and adolescents online.

Slide 30 – Frankie Thomas Case

- **Introduction:**
  - Another tragic example illustrating the severe consequences of unmonitored online activity and lack of appropriate safeguards.
  - Focus on Frankie Thomas, a 15-year-old girl with autism who took her own life in 2017.
- **Case Overview:**
  - **Incident Details:**
    - Frankie Thomas was a student at an independent special school designed to cater to her needs due to her autism.
    - Despite being at school for the whole week, she only attended 1 or 2 lessons weekly.
  - **Use of iPad:**
    - The school provided her with an iPad during her time there.
    - On this school-owned and managed device, Frankie accessed various types of content, including suicidal material.
- **Key Points:**
  - **Lack of Controls:**
    - The coroner found that the school believed the iPads had parental controls and content filtering, but in reality, there were none.
    - This allowed Frankie to access harmful content freely, contributing to her decision to take her own life later that day.
  - **Vulnerability Awareness:**
    - The school failed to recognise that different children have varying levels of vulnerability online.
    - This lack of understanding and appropriate action contributed to the tragic outcome.
- **Discussion Points:**
  - **Role of Schools:**
    - The importance of schools in providing safe digital environments for all students, especially those with special needs.
    - The need for comprehensive digital safety policies, including effective use of parental controls and content filtering.
  - **Parental Controls and Filtering:**
    - Highlighting the critical role of parental controls and content filtering on devices used by children.
    - The necessity for regular checks and updates to ensure these measures are in place and effective.
  - **Tailored Safeguards:**
    - The need for tailored safeguards to protect students with different vulnerabilities and needs.
    - Ensuring that staff and parents are trained to recognise and address these vulnerabilities and indicators of victimisation appropriately and timely.
- **Preventive Measures:**
  - **Regular Monitoring:**
    - Emphasising the importance of regular monitoring of students' online activities by schools.
    - Implementation of robust digital safety training for staff and students.

    - **Collaborative Efforts:**
        - The role of parents, educators, and policymakers in creating a safer online environment for children.
        - Encouraging open communication between all parties to address and mitigate risks effectively.

Closing Remarks:

- The case of Frankie Thomas underscores the urgent need for rigorous online safety measures in schools.
- Highlighting the importance of understanding and addressing the unique vulnerabilities of each student to prevent such tragedies.
- This case exemplifies that those at most risk online are often those at most risk offline. The next slide will provide evidence to support this point.

Slide 31 – Internet Matters Research: Refuge and Risk

- **Introduction:**
    - Overview of the importance of understanding the intersection of physical vulnerability and online risks.
    - Introduction to Internet Matters' research titled "Refuge and Risk,"[5] which highlights the effects of physical vulnerability on online safety.
- **Key Findings from the Research:**
    - **Physical Vulnerability and Online Risk:**
        - Children who are vulnerable offline due to physical disabilities, mental health issues, or other factors are also at a higher risk online.
        - These vulnerabilities make them more susceptible to cyberbullying, exposure to harmful content, and online grooming.
    - **Statistical Evidence:**
        - The research provides data showing a higher incidence of online risks for physically vulnerable children.
        - Example statistics could include higher percentages of cyberbullying incidents or exposure to inappropriate content among these children.
- **Impact of Online Risks on Vulnerable Children:**
    - **Mental Health Effects:** Exposure to online risks can exacerbate existing mental health issues, leading to increased anxiety, depression, and other psychological effects.
    - **Isolation and Exclusion:** Vulnerable children may feel more isolated and excluded, both online and offline, due to their experiences.
- **Case Studies and Examples:**
    - Highlight specific cases or anecdotes from the research that illustrate the challenges faced by physically vulnerable children online.
    - These examples provide a concrete understanding of the impact of online risks on these children.
        - 23% [of children with eating disorders] said 'someone online tried to persuade me into some form of sexual activity I did not want'. Almost a third said their nude image was shared in revenge by a former partner after a breakup.
        - "because of my life online (…) 'I forget to eat then eat a lot and then feel bad'"
        - (noting that eating disorders can be a symptom of trauma or post-traumatic stress disorder)
- **Recommendations from Internet Matters:**
    - **Enhanced Safeguarding Measures:** Implementing stronger digital safeguarding measures tailored to the needs of physically vulnerable children.

[5] Internet-Matters-Refuge-And-Risk-Report.pdf (internetmatters.org).

- **Parental and Educational Support:** Providing resources and training for parents and educators to better support and protect these children online.
    - **Policy and Advocacy:** Encouraging policymakers to consider the unique needs of vulnerable children in digital safety regulations and initiatives.
- **Discussion Points:**
    - How can schools and parents work together to mitigate these risks?
    - What additional resources and tools are available to support vulnerable children online?

Closing Remarks:

- Emphasise the importance of continued research and proactive measures to protect physically vulnerable children online.
- Highlight that addressing these issues requires a collective effort from parents, educators, policymakers, and the tech industry.

Slide 32 – Vulnerability Amplification in Online Spaces

Slide Content:

- Highlight each horizontal bar representing physical vulnerabilities.
- Explain the amplification of online risks for physically vulnerable children.

Key Points to Cover:

- **Diagram Overview:**
    - Each horizontal bar represents a specific physical vulnerability.
    - Coloured blocks indicate the percentage of children with that vulnerability experiencing particular online risks.
- **Examples of Online Vulnerabilities:**
    - **Dark Green:** Percentage of children who meet up with someone they met online.
    - **Purple:** Percentage of children who use pornography.
- **Amplification of Risk:**
    - The diagram illustrates the heightened online risks for physically vulnerable children.
    - Emphasise how physical vulnerabilities can lead to increased exposure to online dangers.
- **General Vulnerability:**
    - Clarify that children without physical vulnerabilities are not immune to online risks.
    - Highlight that all children can face online threats, but those with physical vulnerabilities are at greater risk.

Talking Points:

- **Introduction:** Introduce the diagram as part of Internet Matters' research on online risks for vulnerable children.
- **Explaining the Diagram:**
    - "Each of these horizontal bars represents a particular physical vulnerability, such as autism or mental health difficulties."
    - "The different coloured blocks within each bar show the percentage of children with that vulnerability who face specific online risks."
- **Specific Vulnerability Examples:** "For example, the dark green block shows the percentage of children who meet up with someone they met online, while the purple block indicates those who use pornography."
- **Amplification of Risks:** "What this diagram clearly shows is the amplification of risk online for children with physical vulnerabilities. These children are more likely to experience various online threats compared to their peers without these vulnerabilities."

- **Universal Risk:** "It's important to note that while physically vulnerable children face higher risks, no child is completely safe from online dangers. This underlines the need for comprehensive online safety measures for all children."

Closing Remarks: "This visual representation underscores the critical link between physical vulnerabilities and increased online risks. It serves as a powerful reminder of the need for targeted interventions to protect the most vulnerable children in our society."

By following these notes, you can effectively convey the significant amplification of online risks for physically vulnerable children, while also emphasising the universal nature of online threats.

Slide 33 – Percentage of Children Exposed to Various Online Risks

Overview: This slide presents data from Global Kids Online[6], showing the percentage of children in different countries who have been exposed to various online risks. The data highlights the global nature of these issues and underscores the importance of addressing online safety for children across different regions.

Key Points:

- **Self-Harm Content:**
  - Albania: 18%
  - Bulgaria: 18%
  - Chile: 15%
  - Ghana: 15%
  - Italy: 22%
  - Philippines: 14%
  - South Africa: 18%
  - Uruguay: 22%
- **Suicide Content:**
  - Albania: 12%
  - Bulgaria: 12%
  - Chile: 12%
  - Ghana: 16%
  - Italy: 13%
  - Philippines: 20%
  - South Africa: 18%
  - Uruguay: 16%
- **Hate Speech:**
  - Albania: 10%
  - Bulgaria: 28%
  - Chile: 21%
  - Ghana: 12%
  - Italy: 35%
  - Philippines: 12%
  - South Africa: 34%
  - Uruguay: 35%

[6] Done right, internet use can increase learning and skills | Global Kids Online.

- **Violent Content:**
  - Albania: 35%
  - Bulgaria: 26%
  - Chile: 30%
  - Ghana: 18%
  - Italy: 33%
  - Philippines: 30%
  - South Africa: 33%
  - Uruguay: 40%
- **Sexual Content:**
  - Albania: 16%
  - Bulgaria: 37%
  - Chile: 24%
  - Ghana: 39%
  - Italy: 27%
  - Philippines: 22%
  - South Africa: 51%
  - Uruguay: 36%

Discussion Points:

- **Global Perspective:**
  - The data illustrates that children worldwide are exposed to a range of online risks, regardless of their geographic location.
  - Different regions show varying levels of exposure to specific types of harmful content.
- **Implications for Online Safety:**
  - Understanding these statistics is crucial for developing targeted interventions and educational programs to protect children online.
  - Highlight the need for international collaboration in addressing these issues and sharing best practices.
- **Engage the Audience:**
  - Encourage reflections on the differences between countries and discuss potential cultural, economic, or regulatory factors that might influence these variations.
  - Invite questions and discussions on how this data can inform local and global strategies to improve online safety for children.

Conclusion: The data from Global Kids Online emphasises the universal nature of online risks faced by children and the urgent need for comprehensive measures to safeguard their online experiences.

Slide 34 – National Aspects

[Placeholder for the national trainer to add relevant information.]

5.1 ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Slide 35 – Online Child Sexual Exploitation and Abuse

General Introduction

Given the critical focus of our project on Online Child Sexual Exploitation and Abuse (OCSEA), this section aims to provide a comprehensive understanding of the different facets of OCSEA.

We will delve into the following key areas:

- **Child Sexual Abuse:**
    - Examining the prevalence and impact of child sexual abuse facilitated through online platforms.
    - Highlighting the role of digital technologies in the exploitation and abuse of children.
- **Harmful Sexual Behaviour:**
    - Understanding the types of inappropriate and harmful sexual behaviours that children may exhibit or experience online.
    - Discussing the implications of such behaviours on the mental and physical well-being of children.
- **Threat Assessment:**
    - Evaluating the different threats associated with OCSEA.
    - Understanding how these threats are assessed and the measures taken to mitigate them.
- **Financial Extortion:**
    - Exploring how children are targeted for financial extortion through online interactions.
    - Discussing the methods used by perpetrators to extort money and sensitive information from children.

Key Points to Cover:

- **Introduction to OCSEA:**
    - Definition and Scope of Online Child Sexual Exploitation and Abuse (OCSEA)

      Online Child Sexual Exploitation and Abuse (OCSEA) refers to a range of exploitative and abusive activities that are perpetrated against children and facilitated by digital platforms. The term encompasses various forms of sexual exploitation, including but not limited to, the production, distribution, and consumption of child sexual abuse material (CSAM), online grooming for sexual purposes, live-streamed sexual abuse, and extortion of sexual acts or images under threat. Online and offline abuse are often intertwined: vulnerable children are more at risk of OCSEA, victims are requested to perform sexual acts in real life with the view to use a digital capture of it online, (severe) offline consequences are observed on victims, etc.
    - Scope:
        - Global Reach: OCSEA transcends borders, making it a global issue that demands coordinated international efforts. Perpetrators can operate anonymously from anywhere in the world, often exploiting gaps in jurisdictional laws.

        - Anonymity and Accessibility: The internet offers perpetrators a degree of anonymity, which, coupled with the widespread availability of digital devices, facilitates the live streaming of CSEA, as well as rapid production, dissemination, and consumption of CSAM. The accessibility of children online—through social media, gaming platforms, and communication apps—creates multiple avenues for offenders to approach and groom victims.
        - Complexity of Identification and Prosecution: The digital nature of OCSEA makes detection and prosecution particularly challenging. Some perpetrators use techniques and technologies to evade law enforcement, including encryption, the dark web, and cryptocurrencies, which complicates efforts to trace and identify them.
        - Children often don't see themselves as victims, are scared or ashamed of coming forward, which hinders their identification.
        - Psychological and Social Impact: OCSEA has profound and long-lasting effects on victims, including psychological trauma, social stigmatisation, and disruptions in normal childhood development. The impact extends beyond individual victims, affecting families, communities, and broader society.

        This introduction not only provides a clear definition of OCSEA but also outlines the extensive and multifaceted scope of the issue, setting the stage for a deeper exploration of its various dimensions in the following slides.
    - Importance of addressing OCSEA in the context of increasing internet usage among children.
- **Child Sexual Abuse:**
    - Forms of child sexual abuse online (e.g., grooming, live streaming of abuse).
    - Impact on victims and their families.
    - Legal and ethical considerations.
- **Harmful Sexual Behaviour:**
    - Definition and examples of harmful sexual behaviour online.
    - Psychological and social factors contributing to such behaviour.
- **Threat Assessment:**
    - Frameworks and methodologies for assessing threats related to OCSEA.
    - Role of law enforcement and child protection agencies in threat assessment.
- **Financial Extortion:**
    - Mechanisms of financial extortion involving children.
    - Case studies and real-life examples.
    - Preventative measures and parental guidance.

Conclusion: This section will provide foundational knowledge on the various dimensions of online child sexual exploitation and abuse. Each area will be explored in detail, highlighting the challenges, implications, and protective measures associated with OCSEA. The subsequent slides will delve deeper into each of these critical areas, offering insights and strategies to combat these pressing issues.

Slide 36 – Lanzarote Convention: A Comprehensive Framework to Combat Sexual Violence Against Children

Key Points:

- **Purpose:** The Lanzarote Convention is the most comprehensive treaty specifically aimed at the protection of children against sexual exploitation and abuse. It establishes various forms of sexual abuse of children as criminal offences, including those committed within the family, the circle of trust or using coercion.
- **Implementation and Monitoring:** The Convention mandates State Parties to adopt specific legislation to prevent, protect, and prosecute cases of child sexual abuse and exploitation. A dedicated committee, the Lanzarote Committee, is tasked with monitoring the effective implementation of the Convention and identifying best practices among State Parties.

- **Global Reach:** The Lanzarote Convention extends the possibility of accession to any country worldwide, highlighting its global approach to protecting children from sexual violence.
- **Legal and Practical Measures:** The Convention emphasises the creation of a safe environment for children, both in the physical and digital realms, by incorporating measures against grooming and other online risks.

This Convention reflects a robust commitment by States Parties to safeguard children's rights and ensure a holistic legal and social approach to combating child sexual exploitation and abuse in both physical and digital environments.

Slide 37 – The Lanzarote Convention

Presenter Notes:

The Lanzarote Convention is the most comprehensive international instrument addressing child sexual exploitation and abuse. It outlines key offences and mandates preventive measures, protection mechanisms, and prosecution strategies. Here are the primary offences covered by the Convention:

- **Sexual Abuse (Article 18):** Engaging in sexual activities with a child below the legal age of for sexual activities, including through coercion, force or threats; abuse of a position of trust; or abuse of a vulnerable situation of the child.
- **Exploitation of children through prostitution (Article 19):** Recruiting, causing, coercing or exploiting a child to participate in sexual activities for remuneration.
- **Child Pornography/Child Sexual Abuse Material (Article 20):** Involves the production, offering or making available, distribution, transmission, procurement, possession or knowingly accessing child sexual abuse material.
- **Participation of children in pornographic performances (Article 21):** Recruiting, causing, coercing, profiting from or exploiting children for performances of a sexual nature; or knowingly attending such performances.
- **Corruption of Children (Article 22):** Causing children under the legal age for sexual activities to witness sexual abuse or sexual activities.
- **Solicitation of children for sexual purposes (Grooming) (Article 23):** Intentional initiation of communication, through ICTs, with a child to commit sexual abuse, either online or offline.

The Convention underscores the need for comprehensive legal and policy measures to protect children from sexual exploitation and abuse, both offline and online.

National status of the Convention on the Rights of the Child | OHCHR – *[to be added by the national trainer]*.

Slide 38 – Who are the victims

Introduction:

Presenter notes:

- As per international standards, children are individuals under the age of 18. OCSEA thus refers to abuse committed against people who are under 18 years old.[7]
- Victims can be boys or girls.
- Victims of all ages can be identified: some studies indicate that teenagers may be more affected[8], while others show that prepubescent children are over-represented in CSAM.[9]

Key points[10]

- As explained, children who are vulnerable in real life are often vulnerable online as well. E.g.: a 2023 report from WeProtect reveals that "children from minority or marginalised groups based on their sexual orientation, race, ethnicity, or disability are more exposed to online sexual harm". In addition, victims who have

[7] https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[8] Disrupting Harm – ECPAT, INTERPOL.

[9] https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf

[10] https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf; https://www.weprotect.org/economist-impact-parents-survey/

experienced sexual abuse or other traumas in the past are at higher risk of being revictimized, including in online settings.

- Victims are often chosen in the abuser's close environment (circle of trust).
- Teenagers are less likely to report abuse to adults than younger children.

Conclusion:

- It is important not to separate online and offline abuse.
- Professionals should regularly assess children's vulnerabilities, in order to better detect those at risks and victims.
- Educational efforts should target all children with age-appropriate messages, as well as extend to their parents.

Slide 39 – Grooming

Introduction:

- This slide focuses on grooming: how people may groom children on various platforms online with the view to have them engaging in sexual activity.
- Online grooming is when a person exchanges with a child online, in order to build trust and manipulate the child into participating in sexual activities.

Key points:[11]

- Children can be groomed online, offline or both.
- Online grooming aims to normalize sexual behaviours and engage the child into sexual activities online (with a camera) or offline (real life date), or the sharing of self-generated sexual content.
- To do so, groomers can chat with the child, show pornographic content or sexual content of themselves, scare the child, etc.
- Online, children are often groomed on messaging Apps, social media, dating Apps, or gaming platforms (e.g. Instagram, Facebook, Discord, Whatsapp, Telegram, Grindr, Fortnite, Minecraft, Roblox, VRChat, etc.)[12]
- Groomers are more often adults but can also be children. They can be strangers, pretend to be someone else (including a child), or be known to the child.

Discussion points:

- Encourage the audience to discuss with children the key boundaries they should follow: never agree to in-person meetings without consulting an adult, and never share intimate content online.
- Discuss the importance of being aware of risky apps and websites, as well as understanding children's online behaviours.

Conclusion:

- Conclude by emphasising the importance of maintaining ongoing dialogue with children and understanding the indicators of online child sexual exploitation and abuse (OCSEA) to facilitate the early identification of victims.

Slide 40 – Child Sexual Abuse Material (CSAM)

Presenter Notes:

Introduction:

- Child Sexual Abuse Material (CSAM) represents a severe violation of children's rights and is a significant global issue – often misreferred to as child pornography.

[11] See also: https://inhope.org/EN/articles/the-stages-of-grooming

[12] https://bd9606b6-40f8-4128-b03a-9282bdcfff0f.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf
https://unicri.it/sites/default/files/2022-11/Gaming%20and%20the%20Metaverse.pdf
https://safeonline.global/disrupting-harm/

- The term "Child Sexual Abuse Material (CSAM)" is deliberately used in place of "Child Pornography" to more accurately and sensitively describe the nature of the crime and its impact on victims. The preference for CSAM is rooted in several critical reasons:

    1. Recognition of the Crime's Severity: The term "Child Pornography" is misleading as it may imply a consensual or legal form of pornography, diminishing the seriousness of the crime. In contrast, "Child Sexual Abuse Material" explicitly identifies the material as evidence of criminal activity and abuse, underscoring the gravity of the offense.
    2. Acknowledgment of the Victim's Suffering: Referring to such content as "pornography" can obscure the fact that there is a real child who is being abused and exploited. The term "CSAM" centres the child as a victim of abuse, not as a participant in pornography, highlighting the non-consensual and exploitative nature of the act.
    3. Emphasis on Abuse, Not Content: "Child Pornography" suggests a focus on the content itself, whereas "CSAM" emphasises the abusive and illegal actions that produce such material. The term "CSAM" makes it clear that the issue is about the abuse of children, not the production of any form of "entertainment."
    4. Legal and Social Implications: The use of the term "Child Pornography" can perpetuate harmful misconceptions, potentially leading to reduced public outrage and softer legal penalties. By using "CSAM," the terminology aligns with legal frameworks and international standards that recognise the full extent of the crime, ensuring that it is treated with the seriousness it deserves.
    5. Global Consensus and Best Practices: International organisations, including the United Nations, Interpol, and the Council of Europe, advocate for the use of "Child Sexual Abuse Material" to ensure a consistent, victim-centred approach to addressing this crime. This terminology is part of broader efforts to standardise responses to online child sexual exploitation and to prioritise the protection and dignity of victims. Relevant terms to use when talking about (O)CSEA and their definitions have been gathered by these organizations into the "Luxembourg guidelines" (https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf)

- In summary, the term "Child Sexual Abuse Material (CSAM)" is not just a more accurate description but also a critical tool in reframing the conversation around these crimes. It ensures that the language we use reflects the true nature of the offense, the harm to the victims, and the urgent need for robust legal and social responses.
- This slide highlights the scale and impact of CSAM, emphasising the need for heightened awareness and preventive measures.

Key Points:

- **Definition and Scope:**
    - CSAM refers to any material of sexual nature or used for sexual purpose depicting a child.[13]
    - It includes images, videos, and other digital content produced, shared and/or distributed online.
- **Prevalence:**
    - The problem of CSAM is pervasive, with millions of reports annually.
    - In 2022, the National Center for Missing & Exploited Children analysed 32 million reports of CSAM, highlighting the extensive nature of this issue.
    - CSAM can be found in significant amounts on the clear web, making it accessible to anyone.
- **Reporting and Detection:**
    - Organisations like INHOPE Hotlines[14], the Internet Watch Foundation (IWF), INTERPOL, EUROPOL play a crucial role in detecting and removing CSAM.

[13] "EU Directive 2011/93 refers, in its Preamble, to the fact that '[c]hild pornography frequently includes images recording the sexual abuse of children by adults', but argues that child pornography can also be something broader, by adding '[i]t may also include images of children involved in sexually explicit conduct, or of their sexual organs, where such images are produced or used for primarily sexual purposes and exploited with or without the child's knowledge. Furthermore, the concept of child pornography also covers realistic images of a child, where a child is engaged or depicted as being engaged in sexually explicit conduct for primarily sexual purposes' (Recital Paragraph 8)": Luxembourg guidelines, p. 39: https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf

[14] inhopenetwork_hotlinedirectory.pdf

    - The chart on the slide shows the trends in reports of child imagery over recent years, reflecting an alarming increase.
    - It is important to note that CSAM often depicts real-life sexual abuse of children and is not just an online issue. It indicates that a child is in danger. Therefore, taking action upon detecting CSAM involves more than just removing the material or blocking its circulation; it also requires addressing the underlying abuse and protecting the child, if possible.
    - How to recognise if CSAM is illegal (for reporting purposes): it can be challenging to determine whether an image or a video is illegal, especially since CSAM can cross borders, and laws vary between countries. International standards developed by INTERPOL and used by professionals worldwide can assist in this process. According to these standards, an image or a video is considered illegal everywhere if:
        - It depicts a real prepubescent child
        - AND it shows genital or anal areas, OR sexual activities.

      It does not mean that producing, possessing, or sharing such material is acceptable when the depicted child is a teenager, it might nevertheless help you decide what action to take.

- **Technological Challenges:**
    - Advances in technology, including the dark web and encryption, and the use of P2P have made it easier for perpetrators to share CSAM while evading law enforcement.
    - AI and machine learning tools are being developed to detect and prevent the distribution of CSAM more effectively.
- **Impact on Victims:**
    - The victims of CSAM suffer long-term psychological, emotional, and social consequences.
    - The abuse is often ongoing as images are repeatedly shared and viewed, causing repeated and never-ending trauma.
- **Legal and Protective Measures:**
    - Global co-operation and stringent laws are critical in combating CSAM, as are efforts from the private sector to appropriately regulate usage of their services.
    - Efforts also include harsher penalties for offenders and support systems for victims.
    - Workplaces can also play a significant role in detecting CSAM on work devices.

Conclusion:

- CSAM is a critical issue requiring a multi-faceted approach involving law enforcement, technology, and public awareness.
- Emphasise the need for continued vigilance and action to protect children from such heinous exploitation.

Slide 41 – Child Sexual Abuse Material

Key Points:

- The prevalence of Child Sexual Abuse Material (CSAM) is a significant concern globally.
- Many entities are critical in combating CSAM, i.e. the Internet Watch Foundation (IWF) INHOPE, NCMEC, Thorn, INTERPOL, EUROPOL, national hotlines, and national police.
- Recent data shows a drastic increase in the number of reports and confirmed cases of CSAM.
- 2023 CyberTipline Reports by Country (missingkids.org) – the location of the CSAM content reported to NCMEC
    - Georgia 15,055
    - Moldova 30,972
    - Montenegro 8,490

Detailed Points:

- **Issue and Prevalence of CSAM:**
  - The rise in the availability and distribution of CSAM is alarming, indicating a growing threat to children's safety online.
- **IWF Data and Analysis:**
  - The Internet Watch Foundation (IWF) and WeProtect reported a substantial increase in the number of reports received and confirmed cases of CSAM from 2019 to 2023.
  - In 2023, IWF received 392,660 reports, with a significant portion being confirmed as containing illegal content.
  - There is a notable increase in self-generated content, especially among younger children. The data shows a 1000% increase in imagery involving 7–10-year-olds.
- **Self-Generated Content:**
  - A significant part of the confirmed CSAM is self-generated, often involving children who are coerced or groomed into creating explicit material.
  - The increase in self-generated content poses new challenges for prevention and intervention.

Visual Data:

- **Bar Chart:**
  - The bar chart on the left illustrates the number of reports made to the IWF by year (2019–2023).
  - The middle chart shows the confirmed reports containing illegal content.
  - The right chart highlights the rise in self-generated content, with a significant number involving very young children.

Key Statistics:

- **Reports Received:**
  - 2019: 260,400
  - 2020: 299,600
  - 2021: 361,000
  - 2022: 375,230
  - 2023: 392,660
- **Confirmed Reports:**
  - 2019: 132,700
  - 2020: 153,350
  - 2021: 252,000
  - 2022: 255,570
  - 2023: 275,655
- **Tagged Self-Generated:**
  - 2019: 38,400
  - 2020: 68,000
  - 2021: 182,000
  - 2022: 199,360
  - 2023: 254,070

Important Note: The data highlights a growing issue where younger children, even as young as 7–10 years old, are increasingly represented in self-generated CSAM, underscoring the urgent need for robust protective measures.

Conclusion: This section underscores the grave and escalating issue of Child Sexual Abuse Material, emphasising the critical role of monitoring, reporting, and preventive measures in safeguarding children from online exploitation.

In the course of your professional duties, you may come across the circulation of CSAM involving children under your care, or colleagues. It is crucial to take action while preserving digital evidence to avoid compromising any potential investigations. (this will be detailed in Day 2).

Slide 42 – AI and Child Sexual Abuse Material (CSAM)

Introduction:

- In October 2023, the Internet Watch Foundation (IWF) published a report[15] highlighting the alarming use of AI to create child sexual abuse material (CSAM).
- This small-scale study focused on a single dark web forum, uncovering 10,500 synthetic CSAM images, with 2,500 meeting the UK's legal threshold for CSAM.

Key Findings:

- **Scale of the Issue:** The report demonstrated the significant volume of synthetic CSAM being generated and shared on dark web platforms.
- **Legal Implications:** A substantial number of these images qualify as illegal under UK law, emphasising the seriousness of the threat posed by AI-generated content.
- **Emerging Trends:** The UK Safer Internet Centre reported in November 2023 that children are increasingly using AI and "nudification" apps/services to create CSAM of their peers. These tools digitally remove clothing from images, creating explicit content without the physical act.
- July 2024 update: over 3,500 new AI-generated CSAM uploaded on the same forum since October 2023 (increasingly using images of known CSA victims); more images depict the most severe category of abuse; videos have started circulating (deepfakes); the use of clear web to circulate CSAM is increasing.[16]

Discussion Points:

- **Technological Abuse:** AI, while beneficial in many aspects, is being manipulated for malicious purposes, posing new challenges for child protection.
- **Impact on Victims:** The creation and distribution of synthetic CSAM can have severe psychological and social consequences for the victims, particularly when involving peers.
- **Preventative Measures:** The necessity for robust monitoring and regulation of AI technologies and online platforms to prevent abuse. Importance of educating children in about not sharing images of themselves online (as well as advising parents against sharing images of their children).

Conclusion:

- This issue exemplifies the dark side of technological advancements and the urgent need for comprehensive strategies to combat the exploitation of children through AI.
- Highlight the importance of collaboration between tech companies, law enforcement, and child protection organisations to address and mitigate these risks.

Slide 43 – Live-streaming of child sexual abuse

Introduction:

- Live-streamed CSEA means that the sexual abuse of a child is instantaneously transmitted online to the viewer, who can watch and/or engage while the abuse is occurring.

[15] How AI is being abused to create child sexual abuse material (CSAM) online (iwf.org.uk).

[16] https://www.iwf.org.uk/media/opkpmx5q/iwf-ai-csam-report_update-public-jul24v11.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=July%20Newsletter%3A%20Prevention%20and%20emerging%20threats&utm_campaign=July%202024%20Newsletter
See also: https://www.aru.ac.uk/news/growing%20demand%20on%20dark%20web%20for%20ai%20abuse%20images

- Live streaming is on the rise, especially in developing countries like the Philippines or Madagascar. However, it may happen everywhere, and voluntarily and induced self-produced live-streamed material are the most common forms, with victims frequently found in the US and Europe.

Key points:

- There are 3 types of such abuse[17]: voluntarily self-produced live-streamed material (without coercion), induced self-produced live-streamed material (with coercion or grooming), distant live-streamed material (ordered remotely by an adult viewer and performed by another adult – often across continents).
- It leaves no trace, unless someone deliberately records it, which makes the identification of victims and offenders challenging.
- Perpetrators often possess CSAM.[18]

Discussion point (/exercise – if time allows)

- Identification of child victims of live streaming requires careful attention to signs of OCSEA. What are they?

Conclusion

- This form of OCSEA shows that tech solutions alone may not always prevent or detect such abuse. Therefore, internal mechanisms and procedures for identifying victims should prioritize building trust, observing, and engaging with children.

Slide 44 – Non-consensual pornography: "Revenge Porn Helpline"

This does not just affect children – adults are very much affected too.

Slide Content Overview:

- Highlight the issue of non-consensual sharing of intimate images.
- Emphasise the availability of support for individuals affected.

Presenter Notes:

Introduction:

- This slide focuses on the UK Revenge Porn Helpline, which offers support and advice to individuals who have experienced the non-consensual sharing of intimate images.
- While our primary focus is on child online safety, it's crucial to recognise that online abuse affects people of all ages.

Key Points:

- **Nature of the Issue:**
  - The sharing of intimate images without consent, often referred to as "revenge porn," can cause significant emotional and psychological harm.
  - This type of abuse is not limited to children; adults also face these violations, highlighting the broad scope of online safety concerns.
- **Role of the Helpline:**
  - The UK Revenge Porn Helpline provides confidential advice and support to those affected.
  - The helpline assists individuals in removing non-consensual images from the internet and offers emotional support and guidance on legal options.
- **Statistics and Impact:**
  - Discuss the prevalence of revenge porn cases, if available, and the growing need for such supportive services.
  - Emphasise the importance of raising awareness about the resources available to help victims of this type of abuse.

[17] https://www.datocms-assets.com/74356/1662373940-netcleanreport-2019.pdf

[18] https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Discussion Points:

- Encourage the audience to consider how online safety measures can be improved to protect against the non-consensual sharing of intimate images.
- Discuss the importance of educating young people about the risks and legal implications of sharing intimate images.

Conclusion:

- Conclude by reaffirming the significance of comprehensive online safety and comprehensive sexuality education and the availability of support resources for all age groups.
- Highlight that the issue extends beyond children and affects adults, necessitating a broader approach to online safety and support services.

Slide 45

This diagram represents the number of images reported (and removed) by the Revenge Porn Helpline by gender. On average each case received by the Revenge Porn Helpline from a man had 0.3 images per case, compared to 8.6 for women – a 30-fold increase by gender.

Slide 46 – Introduction to Financial Extortion or 'Sextortion'

- Skip onto next slide

Slide 47 – Sextortion

Introduction to Financial Extortion or 'Sextortion'

Definition:

- **Sextortion** involves coercing individuals into providing explicit images, videos, money, or other favours through threats of exposing their private content. It typically begins with an online interaction where the victim is persuaded or tricked into sharing intimate content, which is then used to blackmail them.

Target Demographic:

- While sextortion can affect anyone, children, young people, and men are particularly vulnerable due to their frequent use of social media and online platforms where they can be targeted. In 2023, the Revenge Porn Helpline reported[19] that 30% of their cases involved sextortion, with an overwhelming 93% of these cases involving male victims.

Mechanisms of Sextortion:

- **Acquisition of Content:** Perpetrators gain access to private images or videos through various means, including hacking, deceit, impersonation, or consensual sharing, which is later exploited.
- **Threats and Coercion:** Victims are threatened with the release of their private material unless they comply with the extortionist's demands, often leading to significant financial and emotional distress.

Impact on Victims:

- **Emotional and Psychological Distress:** Victims often experience severe anxiety, fear, and shame, leading to long-term psychological issues. The stigma associated with sextortion can prevent victims from seeking help, exacerbating their situation.
- **Financial Consequences:** Extortionists typically demand money, leading to financial strain, especially for young victims or their families.

Rising Trend:

- There has been a noticeable global increase in sextortion cases, driven by the widespread use of technology and internet connectivity. Reports of sextortion significantly increased in 2021, and it remained the most reported issue to the Helpline in 2022, highlighting the ongoing and escalating nature of this threat.

[19] revenge-porn-helpline-report-2023.pdf (revengepornhelpline.org.uk).

Preventative Measures and Response:

- **Education and Awareness:** It is crucial to educate young people about the dangers of sharing explicit content and promote safe online behaviours. Open communication between parents, educators, and children about internet safety can help prevent such incidents.
- **Support and Resources:** Establishing support systems, including helplines, counselling, and legal assistance, is essential. Encouraging victims to report sextortion through accessible and anonymous reporting mechanisms without fear of judgment or reprisal is crucial for timely intervention.
- Importance of educating children about not sharing images of themselves online (as well as advising parents against sharing images of their children.)

Conclusion:

- **Call to Action:** Emphasize the importance of collective efforts from parents, educators, doctors, law enforcement, and tech companies to safeguard individuals, particularly children, from sextortion.
- **Available Resources:** Provide information on where victims can seek help and support, stressing the importance of anonymous support services in addressing this growing issue.

Slide 48 – Rise in Sextortion Cases

Introduction to ITV News Clip on Sextortion:

- We will now watch a brief news clip produced by ITV News in April 2024[20].
- This clip highlights alarming new figures about the rise in sextortion victims, particularly targeting students.
- It offers a detailed account of the current sextortion landscape, focusing on the methods perpetrators use and the impact on young victims.
- The clip also features expert commentary and real-life accounts that underscore the severity and pervasiveness of this issue.

Key Points to Look Out For:

- **Statistical Increase:** Pay attention to the statistics showing the increase in reported sextortion cases.
- **Target Demographic:** Note the specific targeting of students and the reasons behind this trend.
- **Expert Insights:** Listen to the insights provided by experts on why sextortion is on the rise and what measures can be taken to combat it.
- **Victim Stories:** Hear from victims who have experienced sextortion, highlighting the personal impact and psychological toll.

[If more suitable clip from relevant state, national trainer may replace and update.]

Slide 49 – National Alert: Financially Motivated Sexual Extortion

- **Context:** The National Crime Agency (NCA) and Child Exploitation and Online Protection (CEOP) Command in the UK have issued an urgent alert to education settings across the country. This highlights the pressing issue of sextortion, specifically targeting children and young people.
- **Content Overview:**
  - **Definition:** Financially motivated sexual extortion (sextortion) involves coercing victims into paying money or meeting other financial demands under the threat of releasing intimate images or videos.
  - **Scale of Issue:** The alert emphasises the significant increase in reported cases globally, involving children being forced into these situations by organised crime groups (OCGs) based overseas.
  - **Victim Demographics:** While sextortion affects all ages and genders, a large proportion of cases involve male victims aged 14–18.

[20] 'They killed our son': Online scammers tearing families apart as sextortion cases soar | ITV News.

- **Action Points for Education Professionals:**
  - **Develop Understanding:** Familiarise yourself with the details of financially motivated sexual extortion by reading this alert and the guidance on sharing nudes and semi-nudes published by the UK Council for Internet Safety.
  - **Referral Process:** If sextortion cases are disclosed or discovered, refer them to local police and/or local authority children's services through your safeguarding procedures.
  - **Supportive Language:** Avoid using victim-blaming language and support children and young people in getting their images removed.
  - **Empowerment:** Educate children and young people on how to safely respond to requests or pressure to provide intimate images or videos, emphasising that the responsibility is not on the child.
  - **Importance of Awareness:** This alert underscores the importance of being vigilant and proactive in safeguarding children against the growing threat of sextortion. It is crucial to integrate these practices into the broader efforts of online safety and child protection.

Conclusion: Highlight the urgency and necessity of being well-informed and prepared to handle cases of sextortion within educational settings. Emphasise the role of educators in safeguarding children and fostering a safe online environment.

Slide 50 – Who are the perpetrators?

Presenter notes:

You can start by asking the audience, "Who do you think perpetrators are?" This question may provide an opportunity to discuss biases.

Key points:

- There is no specific profile for child sex offenders.
- Abusers can be paedophiles, but not always. Paedophilia is a clinical term describing individuals who are sexually attracted to prepubescent children. Hebephilia refers to those who are attracted to pubescent children (teenagers), which may be influenced by myths surrounding virginity. (*Doctors in the room may want to comment on these terms and definitions.*) These terms are not used in the law; the focus is on the criminal behaviour rather than the individual's preferences. Some offenders may be sexually active only with adults and abuse children simply because the opportunity arose, sometimes without realizing the person was underage.
- CSEA perpetrators can be both male and female, although they are predominantly male.
- They can either be adults or children, with an increasing number of children being identified as perpetrators of OCSEA (see the following slides).
- Online just like in real life, perpetrators are often from the child's environment, especially when the abuse involves self-generated material[21]: 60% of online abuse cases involve a perpetrator known to the child (source: Disrupting Harm report[22]).

Discussion point:

- Staff members can also be OCSEA perpetrators. What steps would you take if you discovered that a colleague was storing CSAM on their devices or showing pornographic content to children?

Slide 51 – Harmful Sexual Behaviour

In this section, we will discuss **Harmful Sexual Behaviour (HSB)** among children and young people in the online environment. Understanding HSB is crucial as it encompasses a range of inappropriate or abusive behaviours that children might exhibit or be subjected to online. These behaviours can have severe implications for the emotional and psychological well-being of the affected individuals.

[21] https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf

[22] Disrupting Harm | Safe Online.

Key Points to Cover:

- **Definition and Scope: Harmful Sexual Behaviour (HSB):** Refers to a range of sexual behaviours expressed by children and young people that are developmentally inappropriate, may be harmful to themselves or others, or be abusive towards another child, young person, or adult.
- **Prevalence:**
    - HSB is increasingly recognised in the context of the digital world, where the accessibility and anonymity of the internet can exacerbate these behaviours.
    - Studies and reports indicate a rising trend in the instances of HSB among children, often facilitated by social media, messaging apps, and online gaming platforms.
- **Factors Contributing to HSB:**
    - **Exposure to Inappropriate Content:** Children may mimic behaviours they have been exposed to through pornography or other explicit content online.
    - **Peer Pressure and Social Influence:** Online platforms can amplify peer pressure, leading to the normalisation of harmful behaviours.
    - **Grooming:** Perpetrators may manipulate children into exhibiting or participating in HSB.
- **Impacts of HSB:**
    - **Victims:** Children who are victims of HSB often experience long-term emotional and psychological trauma.
    - **Perpetrators:** Children who exhibit HSB might face social, educational, and developmental challenges, as well as legal consequences, and may need specialised support to address these behaviours.
- **Preventative Measures and Responses:**
    - **Education and Awareness:** Teaching children about healthy relationships (in particular sexuality and consent) and boundaries can help prevent HSB.
    - **Parental and Guardian Controls:** Active supervision and the use of parental controls on digital devices can mitigate exposure to harmful content.
    - **Professional Support:** Access to counselling and psychological support for both victims and perpetrators is essential.

We will now proceed to explore specific examples and case studies to understand the various dimensions of HSB and how they manifest online.

Slide 52 – Everyone's Invited and Ofsted Review of Sexual Abuse in Schools (2021)

Introduction: This section delves into the critical issue of harmful sexual behaviour in educational settings, drawing upon two significant sources: the platform Everyone's Invited and the Ofsted review of sexual abuse in schools and colleges conducted in 2021[23]. Both provide vital insights and underline the pressing need for addressing sexual harassment and abuse among young people.

Everyone's Invited:

- **Platform Overview:**
- **Website:** everyonesinvited.uk
- **Purpose:** Launched to provide a safe space for survivors of sexual harassment and abuse to share their experiences anonymously.
- **Impact:** Amplified voices of thousands, revealing the widespread nature of these issues within educational institutions and beyond.
- **Significance:** Highlights the often-unseen prevalence of sexual misconduct and encourages systemic change within educational environments.

[23] Review of sexual abuse in schools and colleges – GOV.UK (www.gov.uk).

Key Quotes from the Slide:

- *"Sexual harassment and online sexual abuse is so widespread that it needs addressing for all children and young people."*
- **Interpretation:** This emphasises the pervasive nature of sexual harassment and the urgent need for comprehensive measures to tackle it.

Ofsted Review of Sexual Abuse in Schools (2021):

- **Background:** Conducted in response to the testimonies shared on Everyone's Invited.
- **Scope:** Extensive review across various schools and colleges in the UK.
- **Findings:**
  - **Prevalence:** Sexual harassment, including online abuse, is much more common than previously acknowledged.
  - **Recommendations:**
    - Schools and colleges, alongside multi-agency partners, should act proactively against sexual harassment and online abuse.
    - Actions should be taken even in the absence of specific reports, acknowledging the normalised nature of such behaviour among students.
  - **Significance:** The review underscores the necessity for proactive safeguarding measures and the importance of creating a safe educational environment for all students.

Key Quotes from the Slide:

- *"Recommends that schools, colleges and multi-agency partners act as though sexual harassment and online sexual abuse are happening, even when there are no specific reports."*
- **Interpretation:** This highlights the need for a proactive approach in dealing with sexual harassment, recognising that the absence of reports does not equate to the absence of incidents.

Children, particularly girls, routinely received unwanted sexual images and requests for intimate images.

Slides 53 to 55 – Impact of OCSEA on victims (3 slides)

Presenter notes:

You might consider starting by inviting someone in the room to share their experience of speaking with a traumatised victim.

Key points:

- OCSEA is traumatising and may generate trauma and post-traumatic stress disorders, which symptoms include: depression, anxiety, hostility, excessive distrust, feeling of guilt, memory loss, as well as physical symptoms (e.g. headache, eating disorder, etc.).
- These symptoms may influence the victim's behaviour. He/She might be aggressive, refuse to talk, lie, …
- The perpetrator's control over the victim may also impact the victim's behaviour and his/her willingness to come forward.
- In such cases, the victim's behaviour may result in biases, misunderstandings, doubts, or irritation from professionals.
- These symptoms can be used as indicators of OCSEA and help identify victims.

Actions to take:

- The impact of OCSEA on victims must therefore be considered when engaging with them. Professionals should recognize the effects of trauma, exercise patience, tailor their responses to the child, and offer appropriate support (psycho-social and/or legal support, support in getting their images removed…).

- Most importantly: professionals working with child victims should avoid using victim-blaming language, asking too many questions about what happened, confronting the victim and the abuser, commenting on the victim's behaviour, or putting the victim at risk (such as through breaches of confidentiality).

Discussion points

- Interviewing child victims of sexual abuse requires specific skills. Participants may be asked about their ability to conduct such interviews.

Conclusion

- Reponses must be victim-centric and take all these elements into consideration in order not to harm the victim further.

If possible (suggested exercise): role play. 1 person (participant or trainer) acts as the victim reporting abuse (circulation of a recorded live-streamed sexual abuse for example), while another participant acts as a professional (social worker, teacher, or doctor). The other participants can be divided into 2 groups: one group observes and takes notes about how the professional engages with the victim, while the second group takes notes about the proposed response. The results can also be used on the second day when discussing policies and safeguarding mechanisms.

(This exercise can be moved at the end of the training as a wrap-up exercise. In that case, a third group could work on identifying gaps in the online safety measures.)

Slide 56 – WeProtect Threat Assessment

Slide Overview:

- This slide provides a summary of key findings from the WeProtect Global Alliance Threat Assessment on child sexual exploitation and abuse online.
- It emphasises the growing scale and evolving methods of abuse, highlighting the need for comprehensive and coordinated responses.

Key Points to Cover:

- **Escalating Issue:**
  - Child sexual exploitation and abuse online is intensifying both in scale and complexity.
  - New technologies and platforms are being exploited by offenders to target children.
- **Importance of Safety by Design:**
  - Highlight the urgent need for integrating safety measures into the design of digital platforms.
  - Discuss the significance of aligning global internet regulations to create safer online environments.
- **Public Health Approach:**
  - Advocate for adopting public health strategies to prevent violence and abuse.
  - Incorporate insights from children and adopt child-centered approaches to better understand and address the issue. A victim-centric approach includes respect of the "do not harm principle". Professionals should avoid revictimizing children with inappropriate response (as explained earlier).
- **Perpetrators Often Known:**
  - Present the statistic that 60% of online abuse cases involve a perpetrator known to the child (source: Disrupting Harm report[24]).
  - This underscores the importance of educating children about safe online interactions, even with known individuals.
- **Rapid Grooming in Gaming Environments:**
  - Share the data insight that the average time for a child to be groomed in a social gaming environment is 45 minutes, with extreme cases happening in as little as 19 seconds.

[24] Disrupting Harm | Safe Online.

  - Stress the need for vigilance and the implementation of protective measures within gaming and social platforms.

Actionable Insights:

- Encourage adoption of proactive safety measures by tech companies.
- Promote awareness and education for parents, educators, and children on the risks and signs of online abuse.
- Advocate for stronger global collaboration and enforcement of internet safety regulations.

Slide 57 – Image Removal

Both takeitdown.ncmec.org and stopncii.org are initiatives designed to help combat the spread of sexually explicit images online, especially those involving minors or non-consensual sharing. Below is a brief summary of how each platform operates:

TakeItDown (takeitdown.ncmec.org)

Developed by the National Center for Missing and Exploited Children (NCMEC), TakeItDown is aimed specifically at minors who want to have explicit images or videos of themselves removed from the internet. The process is designed to preserve the anonymity of the individual.

How It Works:

- **Submission:** Children can anonymously submit explicit images or videos to TakeItDown.
- **Digital Fingerprinting:** The platform uses technology to create a unique digital fingerprint (hash value) of the content without storing the images or videos themselves.
- **Database Distribution:** These hashes are added to a database that is accessible by participating tech companies.
- **Content Removal:** Companies use these hashes to identify and remove the content from their services, preventing further spread.

StopNCII.org

StopNCII (Non-Consensual Intimate Image) is part of the UK-based Revenge Porn Helpline. It is designed for victims of non-consensual intimate image abuse above the age of 18.

How It Works:

- **Registration and Verification:** Users register and verify their identity to ensure that they are the subjects of the content in question.
- **Hashing:** Users submit images or videos to be hashed; the actual content is not stored.
- **Hash Use:** Similar to TakeItDown, these hashes are shared with technology platforms that use them to detect and remove matching content.
- **Support:** StopNCII also provides advice and support to victims navigating the emotional and legal complexities associated with such abuse.

Summary for Presentation

Both platforms leverage hashing technology to help remove explicit content from the internet without storing or sharing the images or videos themselves. They differ mainly in their target audiences—children for TakeItDown and adults for StopNCII—and in the type of support they offer, reflecting the different legal and emotional needs of these groups. These initiatives represent modern, tech-driven approaches to safeguarding individuals' digital rights and dignity.

Slide 58 – Council of Europe: Integrated Strategies Against Violence Against Children

The Council of Europe Policy Guidelines on Integrated National Strategies for the Protection of Children from Violence aim to be a source of inspiration for states striving to adopt a holistic approach to violence against children and to guarantee their children a childhood free from violence. The guidelines contain detailed proposals on how to develop an integrated national strategy on the rights of the child and the eradication of violence against children. The strategy is defined as a multidisciplinary and systematic framework integrated into the national planning process, rooted in the UNCRC and bringing together all stakeholders.

Objective: To safeguard children from all forms of violence, including sexual abuse in digital environments, through an integrated approach that emphasises prevention, protection, prosecution, and participation.

Key Components and Recommendations:

- **Legal Framework:**
  - Advocate for robust legislative measures underpinning the **Lanzarote Convention** which specifically targets the sexual exploitation and abuse of children, ensuring stringent, clear, and enforceable laws across member states.
  - Encourage countries to adapt their national laws to include digital realms where children may be at risk.
- **Preventive Measures:**
  - Promote educational programs and awareness campaigns aimed at children, parents, and educators to increase understanding of the risks and signs of digital exploitation.
  - Develop tools and resources that empower children to stay safe online.
- **Protection and Support:**
  - Ensure that effective systems are in place for reporting abuse and providing immediate, accessible support and counselling to child victims.
  - Encourage the development of safe digital environments and the use of technological solutions to detect and prevent abuse.
- **Prosecution of Offenders:**
  - Support cross-border co-operation in the prosecution of offenses, reflecting the global nature of the internet.
  - Engage with internet service providers and technology companies to ensure the swift removal of abusive material and the tracing of perpetrators.
- **Participation of Children:**
  - Incorporate the views and experiences of children into policy-making processes to ensure measures are relevant and effective.
  - Promote child advocacy groups and platforms that allow children to express their needs and suggestions for safer digital spaces.

Outcome Goals:

- Strengthen the capacity of all stakeholders involved in child protection to effectively respond to challenges posed by the digital environment.
- Achieve a significant reduction in incidents of child sexual abuse online through collaborative efforts and strong policy frameworks.

Council of Europe's Commitment:

- Demonstrates a commitment to the rights of the child by integrating child protection standards into all aspects of digital policy and practice, aiming for a holistic approach that not only reacts to threats but actively prevents them.

Slide 59 – National Aspects

[Placeholder for national trainer to include national aspects.]

6. RESEARCH EVIDENCE

Slide 60 – Research Evidence

Literary review of published academic research (national and international) into online safety.

Slide 61

Global Kids Online | Children's rights in the digital age[25]

- **Research Platform for Child Online Experiences:** Global Kids Online is an international research initiative that investigates children's online experiences, risks, and opportunities across different countries and cultures.
- **Data-Driven Insights:** The platform provides comprehensive, data-driven insights to inform policies and practices that aim to enhance children's safety and well-being in the digital world.
- **Collaboration and Resources:** It serves as a collaborative space, offering resources, tools, and methodologies to support researchers, policymakers, and practitioners in understanding and improving children's digital lives globally.

Investigating Risks and Opportunities for Children in a Digital World:[26]

- **Balancing Risks and Opportunities:** The report explores how digital technologies present both significant risks and opportunities for children, emphasising the need for protective measures while maximising benefits.
- **Global Research Findings:** It provides insights from global research on children's online experiences, highlighting the diverse ways children engage with digital platforms and the varying impacts on their well-being.
- **Call for Comprehensive Strategies:** The report calls for coordinated efforts from governments, tech companies, and civil society to create safe and empowering digital environments for children worldwide.

Digital 2024 – We Are Social[27]

- **Social Media Milestone:** The number of social media users worldwide has surpassed 5 billion, marking a significant milestone in global digital connectivity.
- **Shifting Usage Patterns:** The report highlights evolving trends in social media usage, including the increasing importance of short-form video content and the growing impact of emerging platforms.

Digital Landscape Insights: The analysis provides key insights into how people are engaging with digital platforms, offering valuable information for businesses, marketers, and policymakers in adapting to the rapidly changing digital environment.

Slide 62 – National research and evidence

[National trainer to add national research and evidence that relates to the issues discussed.]

[25] Global Kids Online | Children's rights in the digital age.

[26] Stoilova, M., Livingstone, S., and Khazbak, R. (2021) Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes. Innocenti Discussion Paper 2020-03. UNICEF Office of Research – Innocenti, Florence.

[27] Digital 2024 – We Are Social UK.

7. SCENARIOS

Slide 63 – Scenarios

Using scenarios, an exercise to discuss the implications on children and how to respond.

Slide 64

- Introduce the session's objectives: understanding the complexities of digital safety and ethical responses.
- Explain the format: participants will be divided into three groups, each tackling one of the scenarios.
- Encourage critical thinking and consideration of both immediate and long-term actions in their responses.

Scenario 1 – Inappropriate Image Sharing Among Peers

Scenario Summary: A girl has sent a naked image of herself to her boyfriend via WhatsApp, and it appears that others in the class now have access to this image.

Discussion Questions:

- What are the immediate steps to ensure the safety and well-being of the girl?
- How would you address the boyfriend and the classmates who have the image?
- What preventive measures can be implemented to educate students about the risks and consequences of sharing intimate images?

Presenter Notes:

- Highlight the importance of a sensitive and confidential approach to support the girl.
- Discuss the legal implications, including child protection laws and policies against distribution of such content.
- Suggest involving school counsellors and possibly law enforcement if deemed necessary.
- Emphasise educational initiatives like digital citizenship programs to prevent such incidents.
- Remind the need for a victim-centric approach.
- Discuss how this incident should be communicated (to parents, the media…).

Scenario 2 – Circulation of Pornographic Images of School Staff

Scenario Summary: Pornographic images reported to be of school staff are circulating amongst children.

Discussion Questions:

- What are the steps to control the spread of these images?
- How should the school support the staff member(s) involved?
- What disciplinary actions are appropriate for the students sharing the images?

Presenter Notes:

- Stress on immediate actions to stop further circulation (engaging IT staff, instructing students to delete images, etc.).

- Discuss the support mechanisms for the affected staff, including legal and psychological assistance.
- Consider the need for a clear communication strategy to handle rumours and maintain the dignity of all involved.
- Consider involving school counsellors for children if deemed necessary.
- Investigate why these images are circulating. Has the staff shared them with children? / and actions to be taken if that is the case.

Scenario 3 – Use of Nudification Technology

Scenario Summary: A boy has used a nudification app to create and share intimate images of girls and shared with his friends.

Discussion Questions:

- How to address the misuse of technology in creating non-consensual intimate images?
- What are the implications for the boy who created and shared the images?
- How to support the victims and address the school community's response?

Presenter Notes:

- Focus on the serious nature of creating and distributing "synthetic non-consensual intimate images", stressing legal consequences.
- Suggest immediate supportive measures for the victims and restorative practices if appropriate.
- Highlight the need for incorporating information on emerging digital risks in the school's digital literacy curriculum.

Scenario 4 – Sextortion creating anxiety

Scenario Summary: A child visits your surgery complaining of sleep issues. During the consultation, they reveal that they are a victim of sextortion. The child appears anxious and hesitant, and they are unsure about what to do next. They fear that explicit images or videos might be shared if they do not comply with the perpetrator's demands.

Discussion Questions:

1. What immediate steps should you take to support the child and ensure their safety?
2. How would you handle confidentiality while involving necessary safeguarding authorities?
3. What are the appropriate referrals and follow-up actions to support the child's mental health and well-being?
4. How can you ensure the child feels safe and supported throughout this process?

Presenter Notes:

- **Immediate Action:** Stay calm, listen without judgment, reassure the child, and document their disclosure.
- **Safeguarding:** Follow safeguarding protocols, e.g. report to child protection services, and consult with relevant authorities.
- **Support:** Arrange mental health support and provide resources on handling online threats.
- **Follow-Up:** Monitor the child's well-being and maintain communication with safeguarding teams to ensure ongoing support.

This scenario helps healthcare professionals consider their role in safeguarding children affected by online exploitation.

Group Feedback and Discussion

Presenter Notes:

- Invite each group to present their proposed solutions and rationale.
- Facilitate a discussion on the varying approaches and what can be learned from each scenario.
- Summarise key takeaways and reinforce the school's commitment to a safe and respectful digital environment.

8. FUTURE TECHNOLOGIES

Slide 65 – Future Technologies

Looking forward, a look at emerging technology, particularly GenerativeAI and the potential risks to children – what will participants need to consider into the future to protect them?

Slide 66 – Artificial Intelligence

- **What is Generative Artificial Intelligence?**
  - Define GenAI as a branch of artificial intelligence that focuses on creating new content, ranging from text and images to sounds and videos. It utilises learned patterns and data to generate outputs that are novel and coherent.
  - Emphasise that unlike traditional AI which is primarily analytical, GenAI is creative, enabling it to produce entirely new pieces of content based on its training data.
- **Core Mechanisms of GenAI:**
  - **Learning from Data:** Explain that GenAI models are trained on large datasets. This training involves absorbing vast amounts of information to understand structures, nuances, and relationships within the data.
  - **Pattern Recognition and Prediction:** Detail how these models use statistical techniques to recognise patterns and predict likely outcomes. This capability is what allows GenAI tools to generate content that is contextually relevant and often indistinguishable from human-created content.
  - **Neural Networks:** Introduce neural networks as the architecture most commonly used in GenAI. These are inspired by the human brain and designed to replicate its pattern-recognition abilities. Layers of nodes (neurons) work together to analyse inputs and produce outputs.
- **Examples of GenAI in Action:**
  - Provide examples to illustrate GenAI applications:
    - Text generation models like GPT (Generative Pre-trained Transformer) for writing assistance.
    - Image generators like DALL-E that create images from textual descriptions.
    - Music synthesis systems that compose music based on various genres and styles.

Conclusion:

Sum up by reinforcing that GenAI represents a significant leap in AI's capabilities, shifting from understanding and analysing data to being able to creatively generate new content that mimics human quality and creativity.

This introduction sets the groundwork for understanding the basic functionality and technology behind Generative Artificial Intelligence, providing a clear foundation before delving into deeper discussions on its applications and ethical considerations.

Slide 67 – ChatGPT

Firstly invite delegates to name to logo

How many have used it?

Meet ChatGPT: A Milestone in Conversational AI

Presenter Notes:

- **Overview of ChatGPT:**
  - Define ChatGPT as a state-of-the-art language model developed by OpenAI, which is based on the Generative Pre-trained Transformer (GPT) architecture.
  - Explain that ChatGPT is designed to generate human-like text responses in a conversational manner. It can understand and generate responses based on the context of the conversation, making it highly effective for a wide range of applications from customer service to content creation.
- **Development and Training:**
  - ChatGPT is trained using a variant of machine learning techniques known as unsupervised learning, where the model is fed a massive amount of text data and learns to predict the next word in a sentence.
  - The training process involves adjusting internal parameters to minimise the difference between predicted and actual text sequences, enhancing its ability to generate coherent and contextually appropriate responses.
- **Capabilities of ChatGPT:**
  - Highlight its proficiency in handling diverse topics, from simple factual questions to complex discussions involving reasoning, advice, and creative content generation.
  - Note its ability to maintain a dialogue over several turns, remember the context of the conversation, and provide responses that are contextually relevant.
- **Use Cases:**
  - Briefly mention common use cases of ChatGPT including virtual assistance, educational tools, creative writing aid, and more. ChatGPT has been integrated into various consumer applications to enhance user interaction through natural language understanding.
  - From OCSEA perspective, it could be used to support the grooming of children, as an example
    - Prompt: "turn this sentence into teen language: 'Hi, how are you? would you like to chat with me? what are your hobbies?'"
    - A: "Hey! What's up? Wanna chat? What are you into these days?"
    - Prompt: "turn the same sentence into chat language"
    - A: "hey! how r u? wanna chat? what r ur hobbies?"
- **Interactive Segment:**
  - Invite participants to indicate whether they have used ChatGPT or similar AI-driven tools. This can segue into a discussion on first-hand experiences and observations with the technology.

Conclusion:

- Summarise by stating that ChatGPT represents a significant advancement in the field of artificial intelligence, showcasing the potential of generative models to transform digital interactions.

This slide will provide a foundational understanding of ChatGPT, setting the stage for further discussions on its implications and applications in various sectors.

Slide 68 – Comprehensive Overview of Generative AI Technologies

Title: Unveiling the Capabilities of Generative AI Across Different Media

Presenter Notes:

- **Text Generation: ChatGPT, Gemini, Jasper**

  - **ChatGPT:** Utilises machine learning to simulate human-like text based on prompts, useful for tasks such as conversation simulation, content creation, and problem-solving.
  - **Gemini:** Similar to ChatGPT, Gemini could be a fictional representation of industry-specific text generation tools, demonstrating tailored solutions.
  - **How it works:** These models predict the probability of each subsequent word based on the words that came before, fine-tuning responses from vast datasets of text.
- **Image Generation: DALL-E, MidJourney, Stable Diffusion**
  - **DALL-E:** Generates images from textual descriptions, blending abstract concepts creatively.
  - **MidJourney:** Focuses on creating high-quality artistic images for creative industries.
  - **Stable Diffusion:** A deep learning model that allows users to create detailed images from textual descriptions, accessible to broader audiences.
  - **How it works:** These models use versions of neural networks that understand and interpolate visual data, turning textual descriptions into complex images through learned associations.
- **Video Generation: Runway SORA, Synthesia, Deepfake Technology**
  - **Runway SORA:** Specialises in AI-driven video editing and effects.
  - **Synthesia:** Creates customised video content from text, including virtual avatars delivering speeches or presentations.
  - **Deepfake Technology:** Enables the creation of convincingly real video and audio recordings.
  - **How it works:** These technologies analyse existing video patterns to synthesise new content that matches specified inputs, often employing deep learning to ensure realism and coherence.
- **Voice Synthesis: ElevenLabs, Descript's Overdub, Google Duplex**
  - **ElevenLabs:** Produces realistic voice audio from text.
  - **Descript's Overdub:** Allows the creation of custom voiceover content from typed text.
  - **How it works:** Voice synthesis models convert text into lifelike spoken audio, using intonations and rhythms learned from speech data.
- **Music Generation: AIVA, Amper Music, Google Magenta**
  - **AIVA:** Composes symphonic music using AI.
  - **Amper Music:** Allows users to create soundtracks based on set moods and styles.
  - **Google Magenta:** Explores the role of AI in creating engaging art and music.
  - **How it works:** These systems analyse music theory and structures to compose new music pieces, learning from a vast array of existing musical compositions.
- **Code Generation: GitHub Copilot, Codex by OpenAI**
  - **GitHub Copilot:** Provides code suggestions directly in the IDE based on the user's context.
  - **Codex by OpenAI:** Powers natural language to code generation, helping developers by suggesting entire lines or blocks of code.
  - **How it works:** These models leverage the structure and syntax of programming languages, suggesting or generating code snippets based on best practices and learned patterns.
- **3D Modeling: Runway, NVIDIA's Omniverse, Google Dream Fusion**
  - **Runway:** Offers creative tools for 3D and machine learning applications.
  - **NVIDIA's Omniverse:** A platform for building and operating metaverse applications, including realistic 3D simulations.
  - **How it works:** These tools utilise advanced AI to interpret, model, and render 3D environments from various inputs, applying complex algorithms to simulate realistic textures, lighting, and physics.

Conclusion:

- Conclude by emphasising the transformative potential of GenAI across various fields, enabling both creativity and efficiency. Highlight that these technologies are continuously evolving, broadening the scope of what can be automated or enhanced by AI.

This slide provides a robust introduction to the diverse functionalities and mechanisms behind Generative AI technologies, demonstrating their impact across multiple media and industries.

Slide 69

Invite participants to look at this perfectly normal image and to see if they can spot anything unusual.

Lady in the middle has 3 legs. Hands and fingers look unusual. This was a synthetic image created in November 2023.

Detecting Anomalies in Synthetic Images

Presenter Notes:

- **Introduction to Anomalies in Synthetic Images:**
  - Explain that anomalies such as unrealistic physical features or impossible objects (like a person with three legs) are common in synthetic images. These anomalies can occur due to errors in the AI's understanding of human anatomy or the merging of multiple images.
- **Highlighting the Specific Anomaly:**
  - Direct the audience's attention to the anomaly of the third leg in the image. Discuss how such errors provide clear evidence of image manipulation or synthetic generation.
  - Use this opportunity to engage the audience, asking if anyone noticed the anomaly before it was pointed out, fostering a discussion on observation skills.
- **Technical Explanation:**
  - Provide a brief explanation of why these anomalies occur, particularly focusing on the limitations of current AI technologies like GANs which might not perfectly understand or replicate the nuances of human forms and spatial relationships.
- **Interactive Analysis:**
  - Encourage the audience to think about other areas in the image that might look 'off' or discuss how the anomaly impacts the overall perception of the image's authenticity.
- **Ethical Discussion:**
  - Use this anomaly as a springboard to discuss the ethical implications of using synthetic images. Talk about the potential for misuse in various contexts and the importance of transparency in media.
- **Conclusion:**
  - Summarise the importance of critically assessing images in the digital age where AI-generated content is becoming more common. Highlight the skills needed to identify such anomalies and the ethical considerations in using synthetic imagery.

Slide 70 – Sora prompt

Sora is OpenAI's advanced AI model capable of generating realistic videos from text prompts. This model can create complex scenes reflecting detailed instructions, simulating the physical world in motion. Sora supports video generation up to a minute long, maintaining high visual quality and fidelity to the provided prompts. It's designed to understand and execute complex visual storytelling, making it an innovative tool for creatives in various fields such as filmmaking and digital art. Currently, Sora is in the testing phase, where it is being evaluated for potential risks and improvements.

Slide 71

Example from Sora. Reminder that this is entirely synthetic. This person doesn't exist and this location doesn't exist. It is possible to identify that this is synthetic – her feet seem to float on the surface of the pavement.

Slide 72 – GenAI Considerations

- **Ethical Considerations:**
  - GenAI raises significant ethical concerns regarding the autonomy and rights of individuals, especially when used in surveillance or decision-making processes that lack transparency.
  - The creation of deepfakes or manipulated content can lead to misinformation and impact societal trust, requiring strict ethical guidelines to manage its use responsibly.
- **Bias in AI Systems:**
  - AI models can reflect or amplify biases present in their training data, leading to discriminatory outcomes in areas such as hiring, law enforcement, and loan approvals.
  - Addressing bias involves diversifying training datasets and implementing fairness-aware algorithms to ensure equitable treatment across different demographics.
- **Security Risks:**
  - AI systems are susceptible to adversarial attacks where slight, often imperceptible inputs can deceive the models into making incorrect decisions.
  - Security measures need to include robust adversarial training, continuous monitoring, and updating of AI systems to defend against such threats.
- **AI Hallucinations:**
  - AI hallucinations occur when models generate false or irrelevant information, which can be problematic in applications requiring high accuracy such as medical diagnosis or journalistic reporting.
  - Strategies to mitigate hallucinations include improving model architecture, fine-tuning with accurate data, and implementing rigorous validation checks.
- **Plagiarism and Originality Issues:**
  - GenAI can replicate and produce content that closely resembles existing works, posing challenges for copyright and originality.
  - Developing systems to track AI-generated content's lineage and integrating plagiarism detection tools are vital for maintaining integrity and crediting original creators.
- **Data Cannibalism:**
  - This phenomenon involves AI models consuming and retraining on their outputs, potentially leading to feedback loops that degrade the quality of information produced.
  - Preventing data cannibalism requires careful design of data pipelines and checks to ensure that outputs do not recursively influence the training process without oversight.

Conclusion:

Conclude by highlighting the necessity of a multidisciplinary approach in addressing these challenges, involving policymakers, technologists, and ethicists to ensure that GenAI technologies are developed and deployed in a manner that is safe, fair, and beneficial for society.

Slide 73 – Online Nation 2023 Report

The "Online Nation 2023" report[28] by Ofcom provides an extensive overview of digital trends in the UK, covering internet usage, online platforms, and digital behaviours. The research examines how individuals and businesses engage with online services, focusing on aspects such as social media use, streaming habits, e-commerce, digital

[28] Online Nation 2023 Report (ofcom.org.uk).

advertising, and the regulatory landscape. This analysis highlights changing patterns in digital consumption and the evolving roles of different platforms in daily life. This serves as a useful comparison point for understanding similar trends in other regions.

Slide 74

The "Online Nation 2023" report by Ofcom provides insights into the usage of generative AI systems among different age groups in the UK. Here's a summary of the key findings regarding who is using generative AI systems and how:

- **Primary Users:**
  - **Generation Z (Teens and Younger Children):** This group is significantly more engaged with generative AI technologies compared to other age groups. Specifically, 79% of online teenagers aged 13–17 and 40% of younger children aged 7–12 are using generative AI tools.
  - **Adults:** Adults show more reluctance, with only 31% of internet users aged 16 and above using generative AI. Among those who haven't used these technologies, nearly one in four adults isn't aware of what generative AI is.
- **Usage Experiences and Applications:**
  - **Social and Entertainment:** The most popular generative AI tool among children and teens is Snapchat My AI, especially among teenage girls. This tool has become widely accessible and is primarily used for social interactions and entertainment.
  - **Educational and Creative Uses:** Generative AI is also used for educational purposes, such as helping with homework, and for creative tasks like writing poetry, creating artwork, and even coding.
  - **General Curiosity and Exploration:** Many users, particularly teens, explore the capabilities of generative AI out of curiosity, which includes chatting with AI, finding information, and seeking advice.
- **Concerns and Perceptions:**
  - Despite the high usage rates, there is a strong awareness of the potential risks associated with generative AI. Over half of the users express concerns about its future impact on society, especially the younger users (aged 16–24), who are also the most prolific users and the most concerned about its societal implications.

These insights from the "Online Nation 2023" report illustrate the varied applications and the mixed perceptions towards generative AI across different age demographics, highlighting a landscape where young users are pioneers but also cautious about the technology's broader implications.

Slide 75

This slide presents data from Ofcom's Online Nation 2023 Report, focusing on the usage of generative AI tools by UK internet users aged 16 and above. The table breaks down the percentage of users who have engaged with various generative AI tools, with a further split between male and female users.

Key Points:

- **Overall Usage of Generative AI Tools:**
  - **ChatGPT** is the most used generative AI tool, with **23%** of all internet users engaging with it.
  - **Snapchat My AI** follows with **15%**, then **Bing Chat** at **11%**.
  - Both **DALL-E** and **Google Bard** have a usage rate of **9%**, while **Midjourney** is used by **8%** of the respondents.
- **Gender Differences in AI Tool Usage:**
  - **ChatGPT** shows the highest disparity with **30%** of male users and **17%** of female users.
  - **Snapchat My AI** is used by **18%** of males and **12%** of females.
  - **Bing Chat** usage is **15%** male and **6%** female.
  - Both **DALL-E** and **Google Bard** are used by **14%** of males but only **5%** of females.

    - **Midjourney** is used by **13%** of males and **4%** of females.

Implications:

- The data suggests a significant gender gap in the usage of generative AI tools, with males more likely to engage with these technologies than females.
- This trend may indicate a need for targeted educational initiatives to encourage more balanced use across genders.

Discussion Points:

- **Why ChatGPT is Leading:** Discuss possible reasons for ChatGPT's popularity, such as its broad application range and ease of use.
- **Gender Disparities:** Explore factors contributing to the gender gap in AI tool usage. Consider discussing societal influences, accessibility issues, or varying interests in technology.
- **Future Trends:** Speculate on how these trends might evolve. Will the gap close as AI tools become more integrated into daily life? What efforts can be made to ensure equal access and usage?

Conclusion: This data from the Ofcom report highlights current patterns in the adoption of generative AI tools among different user demographics. Understanding these trends is crucial for developing strategies to promote equitable access and utilisation of emerging technologies.

Slide 76

This slide presents data from the CHILDWISE summer omnibus 2023 survey[29], highlighting the usage of artificial intelligence (AI) tools among online children aged 7–17. The slide details the overall usage and breaks down the data by age group and gender.

Key Points:

- **Overall AI Tool Usage (Ages 7–17):**
    - **59%** of online children have used at least one AI tool.
    - **Snapchat My AI** is used by **51%** of children, making it the most popular AI tool.
    - **ChatGPT** is used by **24%** of children.
    - **DALL-E** and **MidJourney** have lower usage rates, at **7%** and **6%**, respectively.
- **Age Group Breakdown:**
    - **Ages 7–12:**
        - **40%** have used any AI tool.
        - **30%** use Snapchat My AI.
        - **12%** use ChatGPT.
        - **6%** use DALL-E, and **7%** use MidJourney.
    - **Ages 13–17:**
        - **79%** have used any AI tool.
        - **72%** use Snapchat My AI.
        - **29%** use ChatGPT.
        - **7%** use DALL-E, and **5%** use MidJourney.
- **Gender Breakdown:**
    - **Boys (Ages 7–17):**
        - **59%** have used any AI tool.
        - **48%** use Snapchat My AI.

[29] Generative AI in education: Educator and expert views (publishing.service.gov.uk).

        - **14%** use ChatGPT.
        - **10%** use DALL-E, and **8%** use MidJourney.
    - **Girls (Ages 7–17):**
        - **59%** have used any AI tool.
        - **54%** use Snapchat My AI.
        - **34%** use ChatGPT.
        - **4%** use DALL-E, and **4%** use MidJourney.
- **Detailed Gender and Age Insights:**
    - For children aged **7–12**:
        - Boys: **40%** use any AI tool, **28%** use Snapchat My AI, **9%** use ChatGPT, **6%** use DALL-E, **7%** use MidJourney.
        - Girls: **39%** use any AI tool, **32%** use Snapchat My AI, **12%** use ChatGPT, **3%** use DALL-E, **3%** use MidJourney.
    - For children aged **13–17**:
        - Boys: **78%** use any AI tool, **68%** use Snapchat My AI, **29%** use ChatGPT, **10%** use DALL-E, **5%** use MidJourney.
        - Girls: **80%** use any AI tool, **75%** use Snapchat My AI, **41%** use ChatGPT, **4%** use DALL-E, **3%** use MidJourney.

Implications:

- **High Engagement with AI:** A significant proportion of children, especially teenagers, are engaging with AI tools, highlighting their growing integration into daily activities.
- **Gender Differences:** There are notable differences in AI tool usage between boys and girls, particularly with tools like ChatGPT and Snapchat My AI.
- **Age-Related Trends:** Older children (13–17) are more likely to use AI tools compared to younger children (7–12), suggesting that AI engagement increases with age.

Discussion Points:

- **Impact of AI on Young Users:** Discuss the implications of high AI tool usage among children, including potential benefits and risks.
- **Educational Needs:** Emphasise the need for digital literacy education to ensure children understand how to use AI tools safely and responsibly.
- **Gender Disparity:** Explore reasons behind the gender differences in AI usage and how to address these disparities.

Conclusion: The data from the CHILDWISE summer omnibus 2023 survey indicates that a significant portion of online children are using AI tools, with variations across age groups and genders. Understanding these usage patterns is essential for developing appropriate educational and policy responses to support safe and effective AI engagement among young users.

Slide 77 – Day 1 Close

Slide 78 – Review of Day 1

9. ONLINE SAFETY STRATEGIES FOR EDUCATORS, SOCIAL WORKERS AND DOCTORS

Slide 79

A detailed discussion of what strategies, policies and tools an organisation could have in place to effectively protect children online.

Depending on audience makeup, they could be grouped by profession.

Slide 80 – Overview of the Strategies for educators, doctors and social workers

This comprehensive section aims to equip schools, doctors, social workers, and other professionals with the necessary tools and knowledge to safeguard young people in the digital age. It covers the critical aspects of online safety, including understanding online risks, implementing practical safety strategies, and responding to incidents. The section emphasises the importance of collaborative efforts among educators, parents, children, and professionals in creating a secure online environment. It provides actionable advice, policy recommendations, and resources to promote responsible digital citizenship and protect children from online harm.

Slide 81 – Ownership in Online Safety

Main Points:

- **Collaborative Approach:** Effective online safety strategies require a collective effort from a diverse group of professionals, ensuring sustainability and comprehensive expertise.
- **Role of Online Safety Lead:** While appointing an online safety lead is crucial, the responsibility cannot rest on one individual alone. A successful strategy must be integrated into the whole school culture.
- **Involvement of Young People:** Engaging students in the development of the online safety strategy is essential for its relevance and effectiveness.
- **360 Degree Safe Tool:** This self-assessment system helps schools review and track their online safety policies and practices, promoting collaborative input and ongoing improvement.

Discussion:

- **Collaboration Benefits:** Discuss how a wide ownership of the strategy ensures continuity and broad understanding across the school community.
- **Engaging Students and Parents:** Highlight the importance of including students and parents in shaping online safety policies to ensure they are practical and well-received.
- **Tools for Assessment:** Introduce the 360 Degree Safe tool as a resource for schools to measure and enhance their online safety initiatives.

Conclusion: The page emphasises that a holistic and collaborative approach is essential for embedding online safety into the school culture, ensuring it is not only effective but also sustainable. Engaging all stakeholders, including students, parents, and various staff members, enhances the strategy's impact and relevance.

Slide 82 – Safeguarding and accountability mechanisms / Reporting Routines

Introduction:

- Establish clear internal mechanisms to ensure effective responses to Online Child Sexual Exploitation and Abuse (OCSEA). These should include safe recruitment practices, reporting procedures, evidence preservation (in line with legal requirements), decision-making processes, privacy-respecting communication, and protocols for handling media enquiries.

Main Points:

- **Staff Recruitment Rules:** Conduct thorough background and criminal record checks for all hires. Ensure that individuals with CSEA-related records or suspicions are not employed in roles involving children. Adhering strictly to these rules helps prevent employing individuals who may pose a risk.
- **Active Reporting:** Set up multiple reporting channels (e.g., trusted adults, peer mentors, anonymous online forms) for children and staff to report concerns, ensuring these are accessible and safe.
- **Passive Reporting:** Monitor online discussions involving the school or organisation to identify potential issues early. This includes tracking comments from students and parents.
- **Consistency in Response:** Ensure all reports are handled consistently to maintain trust in the system. A standard procedure reinforces reliability and credibility.
- **Evidence Preservation:** Develop protocols for handling digital evidence carefully to avoid altering metadata. Screenshots are safer than opening files, particularly for CSAM. Follow local laws regarding evidence retention, as staff may not have the authority to retain CSAM even for passing to law enforcement.
- **Victims' Needs and Risk Assessment:** Assess the needs of victims and provide appropriate support, addressing risks such as retaliation and exclusion. Consult parents where appropriate to ensure a comprehensive support network.

National Consultant Input:

- *[National trainer should provide additional details on local frameworks and reporting routines relevant to OCSEA.]*

Discussion:

- **Active Reporting Channels:** Discuss the importance of having varied and accessible reporting routes, such as trusted staff, anonymous forms, and peer mentors.
- **Passive Monitoring:** Explore how monitoring online sentiment can help address concerns proactively.
- **Maintaining Trust:** Emphasise the need for a consistent, transparent response to all reports to build trust.
- **Investigations:** Discuss the pros and cons of conducting internal investigations, particularly when staff are involved.

Conclusion:

- Establishing robust reporting routines, both active and passive, is key to managing online safety. Providing multiple reporting channels and a consistent response helps maintain a safe environment for pupils and staff.

Slide 83 – Online Safety Policy

Main Points:

- **Creating a Safe Environment:** Effective online safety policies are crucial for fostering a safe and supportive environment for students. These policies should be clear, practical, and integrated into the school's culture.
- **Effective Communication:** Policies must be well-communicated to ensure they are understood and respected by students, parents, and staff. Clear communication helps everyone know how to use the internet safely.
- **Clarity and Understanding:** The effectiveness of a policy can be gauged by asking students, parents, and staff about their understanding of proper internet use.
- **Regular Review:** Online safety policies should be reviewed regularly to keep up with rapid changes in technology, risks, and behaviours.

- **Collaborative Approach:** Policy development should involve contributions from children, staff, and the wider school community to ensure broad ownership and relevance.
- **Key Points Dissemination:** Important aspects of the policy should be distilled into summary points and integrated into the school culture through various communication channels.
- **Cross-Referencing Policies:** Online safety should be referenced in related policies such as behaviour, pastoral care, health and safety, and school trips.

Discussion:

Question for small group activities – Do you have online safety policies and acceptable use policies in place? How do you know they are clear, understood and respected by all?

- **Ensuring Policy Effectiveness:** Discuss strategies for making sure that online safety policies are not only comprehensive but also clearly communicated and understood by all stakeholders.
- **Engaging the School Community:** Explore ways to involve students, parents, and staff in the development and dissemination of online safety policies.

Conclusion: Developing clear, well-communicated, and regularly reviewed online safety policies is essential for fostering a safe and supportive online environment. By involving the entire school community and integrating key points into everyday school life, these policies can effectively support a positive and proactive culture of online safety.

Slide 84 – Educate children Curriculum

Introduction:

This slide focuses on the importance of integrating comprehensive online safety education into the curriculum, ensuring children are equipped with the knowledge and skills to navigate digital environments safely, recognise potential risks, and respond appropriately to online threats.

Main Points:

- **Curriculum Design:** The online safety curriculum should be progressive, flexible, relevant, and engaging for students.
- **Teaching Objectives:** Focus on teaching students how to stay safe online, protect themselves from harm, and take responsibility for their own and others' safety.
- **Integration Challenges:** Despite the competition with other curriculum areas, it is essential to integrate online safety, digital literacy, and citizenship into existing subjects.
- **Frameworks and Resources:** Utilise expert schemes and frameworks, such as the UKCIS framework "Education for a Connected World," to help plan and implement the curriculum.

Discussion:

Question for small group activities – Describe how your setting educates children and young people to build knowledge, skills and capability when it comes to online safety? How do you assess its effectiveness?

- **Implementing Frameworks:** Discuss how schools can use established frameworks to structure their online safety curriculum.
- **Integration Strategies:** Explore practical ways to weave online safety topics into various subjects without overwhelming the existing curriculum.

Conclusion: Developing a comprehensive online safety curriculum is crucial for equipping students with the skills to navigate the digital world safely. By integrating online safety education into various subjects and using established frameworks, schools can create an engaging and effective learning experience for students.

Slide 85 – Educate children / Example of curriculum: Summary of the United Nations ITU Sango Resource for Child Online Protection

Overview: The ITU Sango resource[30] for child online protection is a comprehensive guide developed by the International Telecommunication Union (ITU) to safeguard children in the digital world. It addresses various online risks and provides tailored guidelines for children, parents, educators, industry, and policymakers.

Key Components:

- **Children:**
  - **Resources:** The guidelines for children are adapted to different age groups, featuring child-friendly formats like storybooks and workbooks. These resources aim to enhance digital skills, promote safe online behaviour, and empower children to exercise their rights online.
  - **Learning through Stories:** Sango, the Child Online Protection mascot, is used to engage young learners through scenarios and questions that teach them about online rights and safety.
- **Parents and Educators:**
  - **Guidance:** The guidelines help parents and educators understand the risks children face online and create a safe, empowering environment. Emphasis is placed on open communication and ongoing dialogue with children about their online experiences.
  - **Support Systems:** Recommendations include setting up support systems at home and in schools to address online safety concerns promptly and effectively.

Suggested Use Cases:

- **Educational Settings:** Teachers can use the storybooks and workbooks to educate students about online safety in an engaging manner.
- **Parent Workshops:** Schools and community organisations can hold workshops for parents using the guidelines to help them better understand and manage their children's online activities.

The ITU Sango resource serves as a vital tool for various stakeholders, providing a structured approach to protecting children in the digital age while promoting their rights and participation online.

Slide 86 – Professional Development

Main Points:

- **Training Needs:** Professional development in online safety is identified as one of the weakest areas in school provision.
- **Regular Training:** All teaching and non-teaching staff should receive regular (at least annual) training on online safety and response to OCSEA, which can be integrated into broader safeguarding or child protection training.
- **Skill Audits:** Conduct audits to assess staff understanding of online safety, ensuring they are equipped to recognise, respond to, and resolve online safety issues consistently.
- **Advanced Training:** Some staff members should receive more in-depth, accredited training to support their professional development in online safety and response to OCSEA.

Discussion:

Question for small group activities – How do you ensure that all staff receive appropriate online safety / response to OCSEA training that is relevant and regularly up to date?

- **Importance of Training:** Discuss the necessity of ongoing training to keep staff updated on the latest online safety practices and issues.
- **Consistency in Approach:** Highlight the need for a unified understanding and approach to online safety among all staff members.

[30] Children | ITU-COP Guidelines (itu-cop-guidelines.com).

- **Targeted Development:** Address the benefits of advanced training for specific staff to enhance the overall capability of the school in managing online safety.

Conclusion: Investing in regular and comprehensive professional development for all staff members is crucial to maintaining a safe online environment in schools. By ensuring consistent training and providing advanced opportunities for some, schools can effectively manage and mitigate online safety risks.

Slide 87 – Secure Infrastructure

Main Points:

- **Technical Solutions:** Implementing technical measures to protect school systems from external threats and misuse.
- **Filtering:** Schools should use filtering systems to manage access to online content, preventing exposure to illegal or inappropriate content such as child abuse imagery, pornography, and terrorist material.
- **Monitoring:** Effective monitoring systems should alert the school when misuse occurs, prompting timely interventions. This is a critical aspect of safeguarding.

Discussion:

- **Balancing Safety and Access:** Discuss the importance of finding a balance between restricting harmful content and allowing educational access to necessary resources.
- **Proactive Monitoring:** Highlight the need for proactive monitoring to identify and respond to potential issues promptly.

Conclusion: Ensuring a secure digital infrastructure within schools is vital for safeguarding students. Implementing robust filtering and monitoring systems helps manage online content access and detect misuse, contributing to a safer online environment for the school community.

Slide 88 – Swiggle.org.uk – A Child-Friendly Search Engine

Presenter Notes:

Introduction to Swiggle:

- An example of a child friendly search engine – others do exist.
- Swiggle.org.uk is a search engine designed specifically for children, providing a safe and user-friendly online search experience.
- Developed by the South West Grid for Learning (SWGfL), it aims to create a secure browsing environment for young users.

Advantages of Swiggle:

Safety Filters:

  - Swiggle employs advanced safety filters to block inappropriate content, ensuring children are not exposed to harmful material.
  - The search engine actively filters out explicit images, videos, and websites, offering peace of mind to parents and educators.

- **Educational Focus:**
  - The platform prioritises educational content, directing children towards informative and age-appropriate resources.
  - It supports learning by highlighting educational websites, making it a valuable tool for both school and home use.
- **User-Friendly Design:**
  - Swiggle features a simple, intuitive interface tailored to children's needs, making it easy for young users to navigate.
  - The design includes larger buttons and clear icons, facilitating an engaging and accessible user experience.

- **Encourages Safe Browsing Habits:**
    - By using Swiggle, children learn to search the internet responsibly and develop good digital habits from a young age.
    - The search engine also provides tips and guidance on safe internet use, reinforcing digital literacy skills.
- **Parental and Educator Controls:**
    - Swiggle offers tools for parents and teachers to customise the browsing experience, adding another layer of safety.
    - These controls can restrict access to certain websites and monitor search activity, ensuring a controlled and secure online environment.

Conclusion:

- Swiggle.org.uk represents a significant step towards safer internet use for children, combining robust safety measures with an educational focus.
- Encourage parents and educators to integrate Swiggle into their children's daily internet activities to promote a secure and enriching online experience.

Slide 89 – TestFiltering.com

Overview: TestFiltering.com is a tool developed to help schools, organisations, and individuals verify that their internet filters are effectively blocking illegal, harmful, and inappropriate content. The service ensures compliance with guidelines and regulations aimed at protecting users, particularly children, from online dangers.

Key Features:

- **Content Blocking Verification:** The platform tests whether filters are effectively blocking access to illegal content such as child abuse material and terrorism-related content, as well as inappropriate content like pornography.
- **Tracking and Reporting:** Users can track their filter test results over time to monitor the effectiveness and consistency of their internet filtering systems.
- **Automation with TestFiltering+:** This premium service automates the testing process across multiple devices, providing real-time alerts and reports. It ensures continuous monitoring and helps maintain compliance with safety standards.

Use Cases:

- **Schools:** Schools can use TestFiltering.com to verify that their internet filters are protecting students from harmful content, ensuring a safe online learning environment.
- **Organisations:** Companies and institutions can utilise the tool to maintain secure browsing environments for their employees and users.
- **Parents and Guardians:** Individuals can use the service to ensure that home internet filters are effectively safeguarding their children from accessing inappropriate content.

Benefits:

- **Ease of Use:** The service is user-friendly, requiring minimal technical expertise to run tests and interpret results.
- **Proactive Protection:** Automated monitoring helps in promptly identifying and addressing any failures in the filtering system, ensuring continuous protection.
- **Compliance:** Helps organisations and schools comply with regulatory requirements regarding internet safety and content filtering.

Slide 90 – Evaluation

Main Points:

- **Gathering Feedback:** Regularly canvass opinions from various school stakeholders, including students and staff, to ensure the online safeguarding strategy is effective and on the right track. Use short online surveys and tools to gather insights.

- **Assessing Effectiveness:** Evaluate the effectiveness of online safety education by assessing student understanding at key points in their learning journey. Determine if students value the education they receive.
- **Staff Development Needs:** Conduct audits of staff training needs to ensure professional development resources are used effectively and address any gaps in knowledge or skills related to online safety.
- **Tracking Progress:** Utilise tools like the 360 Degree Safe tool to track the school's improvement journey in online safety. This tool helps measure progress, inform strategy adjustments, and maintain records of historical improvements.
- **Promoting Success:** Use data on successful outcomes to promote the online safety strategy. Celebrate achievements and seek accreditation, such as the Online Safety Mark from 360 Degree Safe, to recognise and validate the school's efforts.

Discussion:

- **Feedback Mechanisms:** Discuss the importance of continuous feedback from the school community to refine and enhance the online safety strategy.
- **Measuring Impact:** Explore methods for measuring the impact of online safety education on students' behaviours and attitudes.
- **Professional Development:** Highlight the need for ongoing staff training and development to keep up with evolving online safety challenges.

Conclusion: Regular evaluation of the online safety strategy is essential to ensure its effectiveness and adaptability. By gathering feedback, assessing educational impact, addressing staff training needs, and tracking progress, schools can continuously improve their approach to safeguarding students in the digital environment. Promoting and celebrating successes also helps reinforce the importance of online safety within the school community.

Slide 91 – Safer Internet Day (February 11, 2025)

Overview: Safer Internet Day (SID) is an annual event aimed at promoting safer and more responsible use of online technology and mobile phones, particularly among children and young people. It started in Europe in 2004 and has grown to be celebrated in over 100 countries globally. In 2025, it will take place on February 11th.

Opportunities Presented by Safer Internet Day:

- **Education and Awareness:**
    - **Schools and Educators:** Schools can incorporate SID activities into their curriculum through assemblies, classroom discussions, and special projects focused on internet safety. Resources such as lesson plans, games, and activities are available to facilitate these discussions.
    - **Parents and Guardians:** Parents can use this day to engage in meaningful conversations with their children about internet safety, utilising available resources to guide these discussions and reinforce safe online behaviours at home.
- **Community Involvement:**
    - **Workshops and Events:** Community organisations can host workshops and events to educate the public on safe internet practices. This could include sessions for different age groups, from young children to adults, addressing specific online risks and safety measures.
    - **Collaborative Projects:** Encourage collaboration between schools, local businesses, and community groups to create comprehensive internet safety programs.
- **Industry and Policymakers:**
    - **Industry Initiatives:** Tech companies and online platforms can use SID to launch new safety features, promote existing tools for safe internet use, and engage with their user base on the importance of online safety.
    - **Policy Advocacy:** Policymakers can use the occasion to introduce or reinforce legislation aimed at protecting children online and promoting digital literacy.

- **Personal Development:**
  - **Individuals:** Everyone can participate by educating themselves about the latest online safety tips, reflecting on their internet use, and committing to making the internet a safer place through respectful and responsible behaviour online.
- **Global Engagement:**
  - **International Participation:** SID encourages a global dialogue on online safety, with events and activities that highlight the collective responsibility to create a safer internet. This fosters international cooperation and the sharing of best practices.

Safer Internet Day provides a unique opportunity for individuals, schools, organisations, and policymakers to come together and promote a safer digital world. By leveraging the resources and activities available, participants can contribute to a culture of safety and responsibility online.

For more detailed information, resources, and ways to get involved, you can visit Safer Internet Day's official site (Safer Internet Day).

10. ONLINE SAFETY STRATEGIES FOR PARENTS

Slide 92

An exploration of strategies, tools and resources available for parents to manage their families use of technology and creating the right environment. This section focuses on strategies for engaging parents through presentations, providing trainers with practical techniques to effectively communicate online safety practices, empower parents to protect their children online, and encourage a collaborative approach to digital wellbeing.

Slide 93

In today's digitally-driven world, children and young people are more connected than ever before. While the internet offers vast opportunities for learning, social interaction, and entertainment, it also exposes young users to a range of potential risks, including OCSEA (exposure to inappropriate content, and online predators…), cyberbullying, privacy breaches, etc. It is crucial for parents to understand online safety to help navigate these challenges and protect their children from harm. By being knowledgeable about online risks and safe practices, parents can engage in open and informed discussions with their children, set appropriate boundaries, and utilise tools and resources to create a safer online environment. This proactive approach not only safeguards children's well-being but also empowers them to use digital technologies responsibly and confidently.

This section introduces aspects for all parents to consider. It is meant to be used by the training participants who interact with parents as a tool to support education and empowerment activities. It can also be used as a resource by the participants to train their peers.

Slide 94 – Understanding Home Devices and Their Access Points

Introduction: In today's digital age, homes are equipped with a myriad of connected devices. To ensure effective online safety, it's crucial for parents to have a comprehensive understanding of all these devices and their access points within the household. This section will guide you through identifying and managing these devices, room by room.

Slide Overview:

- **Objective:** Equip parents with the knowledge to identify all connected devices in their home and understand their access points to enhance online safety.

Key Points:

- **Living Room:**
  - **Devices:** Smart TVs, gaming consoles (e.g., Xbox, PlayStation), streaming devices (e.g., Roku, Amazon Fire Stick), smart speakers (e.g., Amazon Echo, Google Home), and connected home security systems.
  - **Access Points:** These devices often connect to the home Wi-Fi network and can be used by multiple family members, including children.
- **Kitchen:**
  - **Devices:** Smart refrigerators, smart ovens, connected coffee makers, and smart lighting systems.

    - **Access Points:** While these devices may seem innocuous, they often connect to the internet for updates and remote control, making them potential entry points for unauthorised access.
- **Home Office:**
    - **Devices:** Laptops, desktop computers, printers, scanners, and routers.
    - **Access Points:** These devices are likely to contain sensitive information and have direct internet access. Ensuring these devices are secure is critical for protecting personal and professional data.
- **Children's Bedrooms:**
    - **Devices:** Tablets, smartphones, laptops, gaming consoles, and smart toys.
    - **Access Points:** Children often use these devices for entertainment and education. It's important to monitor their usage and ensure parental controls are in place to protect them from online risks.
- **Parents' Bedrooms:**
    - **Devices:** Smartphones, tablets, smart TVs, and smart home hubs.
    - **Access Points:** These devices are used for personal communication and entertainment. Ensure strong passwords and privacy settings are enabled.
- **Garage and Outdoors:**
    - **Devices:** Connected car systems, smart garage door openers, and outdoor security cameras.
    - **Access Points:** These devices enhance convenience and security but need to be secured to prevent unauthorised access.

Action Steps:

- **Inventory:** Conduct a thorough inventory of all connected devices in each room. Make a list and note the type of device, its location, and its primary users.
- **Security Review:** Check the security settings of each device. Ensure they have strong, unique passwords and updated software.
- **Access Control:** Implement parental controls and set appropriate access levels for children. Regularly review and update these settings.
- **Network Segmentation:** Consider setting up a guest network for less secure devices and keep your main network for critical devices like computers and smartphones.

Discussion:

- Encourage parents to share their experiences and challenges in managing multiple connected devices.
- Discuss the importance of regularly updating device firmware to protect against vulnerabilities.
- Explore tools and resources available for managing and monitoring connected devices.

Conclusion: By understanding the variety of devices in your home and where access happens, you can create a safer digital environment for your family. Regularly reviewing and updating the security settings of each device is a proactive step towards protecting your household from online threats.

Slide 95 – Understanding the Services Used on Home Devices

Introduction: After identifying the various connected devices in the household, the next critical step is to understand the services that are being accessed on these devices. This helps in ensuring that parents can monitor and guide their children's online activities effectively. This section will guide you through a practical approach to uncovering the services used on each device.

Slide Overview:

- **Objective:** Equip parents with strategies to identify and monitor the online services their children use across various devices.

Key Points:

- **Starting the Voyage:**
  - **Engage with Children:** Begin by engaging with your children. Ask them to show you the apps and websites they frequently use on each device. This not only helps you understand their online habits but also opens up a dialogue about online safety.
- **Popular Services to Look For:**
  - **Social Media:** Facebook, Instagram, Snapchat, Twitter, TikTok
  - **Video Platforms:** YouTube, Netflix, Amazon Prime Video
  - **Gaming:** Xbox Live, Fortnite, Roblox
  - **Messaging Apps:** WhatsApp, Messenger
  - **Music and Entertainment:** Spotify, Apple Music
  - **Educational Apps:** Google Classroom, Khan Academy
  - **Others:** Pinterest, Google Play Store, App Store
- **Account and Login Information:**
  - **Importance of Login Details:** Understanding which services require login information is crucial. This includes knowing usernames and passwords, and setting up parental controls where possible.
  - **Privacy Settings:** Review and adjust privacy settings on these services to enhance security and control over what information is shared and with whom.
- **Regular Monitoring:**
  - **Ongoing Dialogue:** Regularly check in with your children about their use of these services. Encourage them to share any new apps or websites they start using.
  - **Activity Logs:** Use device and service activity logs to monitor usage patterns. This can help in identifying any unusual or potentially unsafe behaviour.
- **Setting Boundaries:**
  - **Usage Guidelines:** Establish clear guidelines for the use of these services, including time limits and appropriate content.
  - **Parental Controls:** Utilise built-in parental control features on apps and devices to restrict access to inappropriate content and manage screen time.

Action Steps:

- **Interactive Session:** Conduct an interactive session with your children where they guide you through their favourite apps and websites. Make it a fun and educational experience.
- **Review Settings:** Together, review the privacy and security settings on each service. Explain the importance of these settings in protecting their personal information.
- **Set Up Controls:** Set up parental controls on devices and services to ensure a safe online environment.

Discussion:

- Share experiences about managing and understanding the services children use.
- Discuss challenges faced in monitoring these services and how to overcome them.

Conclusion: Understanding the services that children access on their devices is crucial for maintaining a safe online environment. By engaging with your children, regularly monitoring their usage, and setting appropriate boundaries, you can help protect them from online risks and promote responsible digital citizenship.

Slide 96 – Understanding and Utilising Online Safety Controls

Introduction: This section focuses on familiarising parents with essential online safety controls to protect their children and family. Given the varied levels of technical expertise, especially among parents in Eastern Europe, clarity and simplicity are paramount. We'll cover family sharing settings, parental controls, password security, antivirus software, and more.

Slide Overview:

- **Objective:** Equip parents with the knowledge and tools to effectively use online safety controls to create a secure digital environment for their family.

Key Points:

- **Family Sharing and Account Management:**
    - **Family Sharing Features:** Explain how family sharing works on platforms like Apple and Google. It allows parents to share apps, music, and more with their children while controlling what content they can access.
    - **User Accounts:** Encourage parents to set up individual user accounts for each family member. This enables tailored access and controls for each user.
- **Parental Controls:**
    - **Device-Level Controls:** Demonstrate how to set up parental controls on various devices, including smartphones, tablets, and gaming consoles. Show where to find these settings on popular devices.
    - **Content Filters:** Discuss how to use content filters to block inappropriate websites and apps. Provide examples from services like YouTube Kids, Netflix, and internet service providers (e.g., BT, Sky, TalkTalk, Virgin Media).
    - **Screen Time Limits:** Explain how to set screen time limits to manage how long children can use their devices each day. Highlight the benefits of balancing online and offline activities.
- **Password Security:**
    - **Creating Strong Passwords:** Emphasise the importance of using strong, unique passwords for each account. Provide tips on creating complex passwords and using passphrases.
    - **Password Managers:** Introduce the concept of password managers, which can securely store and generate passwords. Recommend popular tools like LastPass or 1Password.
    - **Two-Factor Authentication (2FA):** Explain what 2FA is and how it adds an extra layer of security. Encourage parents to enable 2FA on all important accounts.
- **Antivirus and Security Software:**
    - **Importance of Antivirus Software:** Highlight the necessity of using antivirus software to protect devices from malware and viruses. Recommend trusted antivirus programs.
    - **Regular Updates:** Stress the importance of keeping all software and operating systems up to date to protect against security vulnerabilities.
    - **Safe Browsing Practices:** Encourage the use of secure, encrypted connections (look for "https://" in the URL) and caution against downloading files or clicking on links from unknown sources.
- **Utilising Service Provider Tools:**
    - **ISP Parental Controls:** Many internet service providers offer built-in parental controls. Explain how to access and configure these settings through their websites or customer support.
    - **Safe Search Settings:** Demonstrate how to enable safe search features on search engines like Google and Bing to filter out explicit content.

Discussion:

- Share experiences about implementing and managing online safety controls.
- Discuss common challenges parents face and practical solutions to overcome them.

Conclusion: By understanding and utilising the various online safety controls available, parents can significantly enhance the security and well-being of their family's digital environment. Regularly reviewing and updating these settings will help keep children safe as they navigate the online world.

Slide 97 – Understanding and Managing Children’s Online Footprint

Introduction: In the digital age, children leave an online footprint through their internet searches, social media interactions, and other online activities. Understanding what children are searching for, what content they are viewing, and what is being said about them online is crucial for their safety and privacy. This section will guide you through monitoring and managing your child’s online footprint effectively.

Slide Overview:

- **Objective:** Equip parents with the knowledge and tools to monitor and manage their children’s online activities and presence to ensure their safety and privacy.

Key Points:

- **Understanding the Online Footprint:**
  - **Search History:** Explain the importance of knowing what children are searching for online. This includes search engines like Google and child-friendly alternatives like Swiggle.
  - **Browsing History:** Emphasise the need to review the websites and content children visit. This helps in understanding their interests and identifying any potential exposure to inappropriate content.
- **Social Media Presence:**
  - **Profiles and Posts:** Discuss the significance of monitoring children’s social media profiles, posts, and interactions. Highlight how information shared can be permanent and visible to a wide audience.
  - **Privacy Settings:** Teach parents how to adjust privacy settings on social media platforms to control who can see their child’s posts and personal information.
- **Online Reputation:**
  - **Digital Footprint:** Explain how comments, photos, and videos posted online contribute to a child’s digital footprint and can affect their reputation.
  - **Search for Their Name:** Encourage parents to periodically search for their child’s name online to see what information is publicly available and address any concerns.
- **Managing Online Footprint:**
  - **Regular Monitoring:** Recommend regularly checking the child’s search and browsing history. Use built-in browser tools or parental control software to facilitate this.
  - **Educational Conversations:** Engage in conversations with children about the importance of their digital footprint and the long-term impact of their online actions.
  - **Positive Footprint:** Encourage activities that contribute to a positive online footprint, such as creating educational content, participating in positive online communities, and showcasing achievements.

Discussion:

- Share experiences about managing children’s online activities and footprint.
- Discuss challenges faced in monitoring and guiding children’s online behaviour and practical solutions to address them.

Conclusion: Understanding and managing children’s online footprint is vital for protecting their privacy and reputation. By regularly monitoring their online activities, adjusting privacy settings, and engaging in educational conversations, parents can help their children navigate the digital world safely and responsibly.

Slide 98 – Familiarising with Reporting Online Issues

Introduction: Reporting online issues is a critical step in maintaining a safe and respectful digital environment. Parents and children should be aware of how to report harmful content, cyberbullying, and other online safety concerns. This section will guide you through the process of reporting issues across various platforms and highlight key organisations that support online safety.

Slide Overview:

- **Objective:** Equip parents with knowledge and resources to report harmful online content effectively, ensuring swift action and resolution.

Key Points:

- **Platform-Specific Reporting:**
    - **Social Media Platforms:** Each social media platform has its own reporting mechanisms. Familiarise yourself with the process for popular platforms:
        - **Facebook:** Use the "Report" button on posts, profiles, or comments to report inappropriate content.
        - **Instagram:** Tap the three dots on a post or profile and select "Report" to flag content or accounts.
        - **X/Twitter:** Click on the down arrow or three dots on a tweet, then select "Report Tweet" to report harmful tweets.
        - **YouTube:** Click on the three dots under a video, then choose "Report" to flag inappropriate videos.
    - **Gaming and Streaming Services:** Understand reporting tools in gaming services like Xbox Live and streaming platforms like Twitch and Netflix.
- **Key Organisations:** *[UK Examples to be replaced with relevant national examples.]*
    - **Internet Watch Foundation (IWF):** Focuses on removing child sexual abuse content online. Reports can be made directly through their website.
    - **True Vision:** Provides information on hate crimes and online reporting tools.
    - **Action Fraud:** The UK's national reporting centre for fraud and cybercrime, providing a platform to report online scams and fraud.
- **Steps to Report:**
    - **Identify the Issue:** Understand the type of content or behaviour that needs to be reported.
    - **Use Platform Tools:** Utilise built-in reporting tools on the platform where the issue occurs.
    - **Seek Support:** Contact relevant organisations for guidance and support if needed.
    - **Follow Up:** Monitor the situation and ensure the issue is addressed appropriately by the platform or organisation.

Action Steps:

- **Interactive Demonstration:** Provide a live demonstration of how to report issues on popular social media platforms and gaming services.

Discussion:

- Share experiences about reporting online issues and the responses received.
- Discuss challenges faced in reporting and how to overcome them.

Conclusion: Understanding how to report online issues is essential for maintaining a safe digital environment. By familiarising themselves with reporting mechanisms and key organisations, parents can effectively address harmful content and protect their children online.

Slide 99 – Parents as Role Models for Online Behaviour

Introduction: Children often emulate the behaviours they observe in their parents. As digital role models, parents play a crucial role in shaping their children's online habits and attitudes. This section will provoke thought and discussion on how parents' online behaviours influence their children and provide practical strategies for modelling positive digital citizenship.

Slide Overview:

- **Objective:** Encourage parents to reflect on their own online behaviours and understand the importance of modelling positive digital habits for their children.

Key Points:

- **Children Mimic Parental Behaviour:**
  - **Observational Learning:** Explain how children learn behaviours by observing adults. Highlight the significance of parents' online actions as examples for their children.
  - **Consistency:** Emphasise the need for consistency in online and offline behaviours to reinforce positive habits.
- **Positive Digital Citizenship:**
  - **Respect and Kindness:** Encourage parents to demonstrate respectful and kind interactions online. Show how these behaviours set a standard for children.
  - **Privacy and Security:** Discuss the importance of modelling good practices in privacy and security, such as using strong passwords and being cautious about sharing personal information.
- **Managing Screen Time:**
  - **Balanced Usage:** Advocate for balanced screen time. Parents should show that digital devices are tools for learning and entertainment, not distractions from real-life interactions.
  - **Quality Content:** Suggest that parents share high-quality, educational content with their children to promote productive use of screen time.
- **Open Communication:**
  - **Discussing Online Experiences:** Encourage parents to talk openly about their online experiences, including challenges and positive interactions. This fosters a culture of transparency and trust.
  - **Active Listening:** Highlight the importance of listening to children's online concerns and experiences, showing empathy and support.
- **Setting Boundaries:**
  - **Digital Boundaries:** Parents should establish and adhere to digital boundaries, such as no devices at the dinner table or during family time, to promote healthy digital habits.
  - **Role Modelling Boundaries:** When parents respect their own set boundaries, children are more likely to follow suit.

Action Steps:

- **Self-Reflection Exercise:** Ask parents to reflect on their online behaviours and identify areas where they can improve to set a better example.
- **Interactive Discussion:** Facilitate a discussion on common online behaviours and how they impact children. Share experiences and strategies for improvement.

Discussion:

- Share stories and experiences about how parental online behaviour has influenced children.
- Discuss common challenges in modelling positive online behaviour and brainstorm solutions together.

Conclusion: As digital role models, parents have a profound impact on their children's online behaviours and attitudes. By demonstrating respectful, responsible, and balanced online habits, parents can help their children develop into positive digital citizens.

Slide 100 – Managing Screen Time – Guidelines from UK Chief Medical Officers

Introduction: Screen time management is a significant challenge for many parents. The UK Chief Medical Officers have provided practical advice[31] to help parents balance the benefits and negative effects of screen-based activities on children's mental health and well-being. This section will outline key recommendations and strategies to manage screen time effectively.

[31] UK CMO commentary on screen time and social media map of reviews – GOV.UK (www.gov.uk).

Slide Overview:

- **Objective:** Provide parents with actionable advice and strategies for managing their children's screen time based on recommendations from the UK Chief Medical Officers.

Key Points:

- **Precautionary Approach:**
  - **Balance Benefits and Risks:** Emphasise the importance of balancing the benefits of screen use, such as educational content and social connection, with the potential negative effects, such as reduced physical activity and sleep disruption.
- **Screen-Free Mealtimes:**
  - **Face-to-Face Interaction:** Encourage screen-free mealtimes to promote face-to-face conversations and family bonding. Highlight the importance of giving full attention to each other during meals.
- **No Screens Before Bed:**
  - **Sleep Hygiene:** Recommend keeping screens out of the bedroom and avoiding screen use before bed to improve sleep quality. Explain how blue light from screens can interfere with the body's sleep-wake cycle.
- **Taking Regular Breaks:**
  - **Two-Hour Rule:** Advise taking breaks after two hours of continuous screen use to prevent eye strain and promote physical activity. Encourage parents to set timers or use apps that remind children to take breaks.
- **Agree on Boundaries:**
  - **Setting Limits:** Discuss the importance of setting and agreeing on screen time limits and online behaviour guidelines with children. Involve children in creating these rules to ensure they understand and respect them.
- **Lead by Example:**
  - **Modelling Behaviour:** Highlight the role of parents as role models in managing their own screen time. Show children how to balance screen use with other activities by demonstrating good practices themselves.
- **Open Discussion:**
  - **Family Conversations:** Encourage regular family discussions about screen time. Ask questions like, "Is our family's screen time under control?" and "Do screens interfere with our sleep or family time?" to assess and adjust screen habits as needed.

Action Steps:

- **Interactive Exercise:** Facilitate an exercise where parents outline their current screen time habits and identify areas for improvement. Provide a template for setting screen time rules and boundaries.
- **Resource Handouts:** Distribute handouts with the UK Chief Medical Officers' guidelines and tips for managing screen time. Include practical steps and tools for implementation.
- **Q&A Session:** Allow time for parents to ask questions and share their experiences with managing screen time. Offer personalized advice based on specific challenges they face.

Discussion:

- Share success stories of families who have implemented these guidelines and seen positive results.
- Discuss common challenges in reducing screen time and brainstorm solutions as a group.

Conclusion: Effective screen time management is essential for maintaining children's mental health and well-being. By adopting the UK Chief Medical Officers' guidelines and involving children in setting boundaries, parents can create a balanced and healthy digital environment at home.

Slide 101 – Kiko and the Manymes

1. **Overview of the Resource**:
   - "Kiko and the Manymes" is an educational comic book developed by the Council of Europe aimed at teaching children about the concepts of digital identity and online safety.
   - Play video in the PowerPoint.
   - The story follows a young character named Kiko who navigates various online scenarios, helping readers understand the importance of managing one's digital footprints and identities.
2. **Key Themes and Messages:**
   - **Digital Identity Awareness:** The comic emphasizes how actions taken online contribute to one's digital identity and the potential long-term implications of these actions.
   - **Privacy and Data Protection:** It highlights the significance of protecting personal information and being cautious about what is shared on the internet.
   - **Critical Thinking:** Encourages children to think critically about the information they encounter online and the personas they or others present.
3. **Usage in Educational Settings:**
   - The resource serves as a conversation starter for educators and parents to discuss online safety topics with children in an engaging and relatable manner.
   - It can be integrated into lessons about internet literacy, citizenship education, or personal development.
4. **Supporting Activities:**
   - Alongside the comic, there may be accompanying materials such as discussion guides, activities, or questions to reinforce the lessons learned and to facilitate deeper understanding.
5. **Access and Distribution:**
   - The comic book is available in multiple languages and can be accessed freely via the provided link, making it a versatile tool for diverse educational environments.
6. **Importance of the Resource:**
   - Given the increasing digital engagement of children, resources like "Kiko and the Manymes" are vital in equipping young users with the knowledge and skills to navigate the online world safely and responsibly.

Recommendation: Encourage educators and parents to utilise this comic as part of their toolkit for teaching digital citizenship and to foster open discussions about online experiences with children.

11. EXISTING PRACTICE

Slide 102

The opportunity to consider and share amongst participants your existing online safety measures and practice. The session will establish examples of good practice.

Depending on audience makeup, they could be grouped by profession.

Slide 103 – Facilitating a Discussion on Existing Practices for Protecting Children

Introduction: In the next section, we will create a space for participants, including teachers, doctors, and social workers, to share their existing practices for protecting children online and offline. This discussion aims to foster a collaborative environment where professionals can learn from each other's experiences and strategies.

Slide Overview:

- **Objective:** Encourage participants to share their practices, discuss challenges, and learn from each other's experiences to enhance child protection efforts with a focus on OCSEA.

Key Points:

- **Setting the Stage:**
  - **Purpose:** Explain that the purpose of this discussion is to share effective practices and strategies for protecting children in various environments, including schools, healthcare settings, and social services.
  - **Safe Space:** Emphasise the importance of creating a safe, non-judgmental space where everyone feels comfortable sharing their experiences and ideas.
- **Guiding Questions:**
  - **Current Practices:** What current practices do you have in place to protect children in your professional setting?
  - **Success Stories:** Can you share any success stories where these practices effectively protected a child or group of children?
  - **Challenges:** What challenges have you faced in implementing or maintaining these practices?
  - **Innovative Solutions:** Have you developed or adopted any innovative solutions to address specific child protection issues?
- **Facilitating the Discussion:**
  - **Open Floor:** Invite participants to share their practices and experiences one at a time. Encourage active listening and respect for each speaker.
  - **Interactive Dialogue:** Promote an interactive dialogue by asking follow-up questions and encouraging others to respond or add their insights.
  - **Sharing Resources:** Encourage participants to share any resources, tools, or materials they use in their practices.

12. ONLINE SAFETY RESOURCES

Slide 104

Signposting effective online safety resources.

Slide 105

[National trainer to signpost to relevant national online safety resources.]

13. NATIONAL FRAMEWORK

Slide 106

An overview of the specific national prevention, reporting and referral mechanisms, alongside existing protocols for each category of professionals in cases of violence against children.

Slide 107

[National trainer to add national framework references.]

14. SUMMARY

Slide 108 – Summary

A review of all content covered and affording participants the opportunity to ask clarification and consolidation questions.

Slide 109 – Questions and contact details

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

Safe Online

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE