Merton Online Safety Strategy: Supporting Merton's Young People to Stay Safe Online

Date: March 2024

Date	Author	Date Of the Next Review	Sign-off
March 2024	D Crabtree	March 2026	MSCP Protect & Promote Young People Subgroup

Contents

Introduction:

In an increasingly digital world, the internet has become an essential part of young people's lives. As a local authority in England, we recognise the importance of creating a safe online environment for our young residents. This Online Safety Strategy aims to outline our commitment to supporting young people in staying safe online and mitigating the potential risks associated with internet use.

Understanding Online Safety:

Online safety encompasses the knowledge, skills, and practices required to protect oneself and others while using the internet and digital technologies. It involves being aware of potential risks, understanding how to use online platforms responsibly, and recognising the importance of maintaining a positive online presence.

The Importance of Online Safety for Young People:

Young people are particularly vulnerable to the risks of the digital world, including cyberbullying, online predators, exposure to inappropriate content, and potential harm to mental well-being. This strategy aims to empower them with the necessary tools and knowledge to navigate the internet safely and confidently. At the heart of our strategy is building Digital resilience which is the ability to understand when you are at risk online, knowing what to do if anything goes wrong, and being able to recover from difficulties or upsets.

Being Online: The Voice of Merton Young People

For most young people the online environment is a positive space which provides young people with a wealth of information and opportunities for connection across the world. Young people have told us that the benefits of being online are:

- Access to a wide range of knowledge and information which promote independent learning and personal development.
- Access to a wealth of resources for study, travel and connection with others
- The ability to speak to family and friends anywhere in the world.

Young people have also shared some of their worries and concerns:

- The freedom can be worrying and they want help with setting boundaries.
- They are worried about being exposed to worrying things like porn, violent extremism.
- The are worried about harassment and bullying online.
- They are worried about predators and people who want to harm children and young people.
- They are worried about scams and fraudulent adverts.
- They are worried that parents/carers and other adults are not as aware about the online world and struggle to give good guidance and advice or protect young people from the risks

Young people want:

- Clear information and guidance especially on building a good online reputation and digital footprint.
- Information about risks and dangers of being online.
- People (including young people) who are online to be 'good neighbours' and be respectful even when angry and disagreeing with others
- They want people to be aware of and stick to age restrictions which means that children and young people can access the right apps, at the right time (in terms of their age) when young people are ready.
- Protection from predators and those who would want to harm or exploit children and young people.

Approach

To provide guidance and inform front line practitioners to:

- Guide children, young people and others to the best sources of information and support and not duplicate the great range of advice and resources already available.
- Help organisations to develop their own solutions and incorporate the principles and priorities in this strategy into those.
- Identify those young people potentially vulnerable.
- Make sure that risk is assessed and managed effectively.
- Make sure that young people understand their own risks in using online services.

Appendix 1 contains a matrix of resources aimed at Adults, Young People and Professionals.

Challenges and Risks:

Our strategy acknowledges that the digital landscape is continuously evolving, presenting new challenges and risks. These may include emerging social media platforms, online gaming communities, and the rapid development of technology including Large Language Models and Generative AI.

By recognising these challenges, we can stay proactive in adapting our approach to online safety.

The 4Cs classification distinguishes between aggressive, sexual and value risks, as this is helpful in retaining a balanced view of the range of risks that children can encounter.

	Content Child engages with or is exposed to potentially harmful content	Contact Child experiences or is targeted by potentially harmful *adult* contact	Conduct Child witnesses, participates in or is a victim of potentially harmful *peer* conduct	Contract Child is party to or exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	**Privacy violations** (interpersonal, institutional, commercial) **Physical and mental health risks** (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) **Inequalities and discrimination** (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

https://core-evidence.eu/posts/4-cs-of-online-risk

The risks that young people face online include:

1. **Cyberbullying and Online Harassment:** Cyberbullying refers to the use of digital communication tools, such as social media, messaging apps, or online forums, to harass, intimidate, or humiliate others. Young people may be targeted through hurtful messages, spreading rumours, or sharing embarrassing content, which can lead to severe emotional distress and even long-term psychological harm.
2. **Online Predators:** The internet provides a platform for individuals with malicious intent to groom and exploit young people. Online predators may pose as peers, gaining trust and manipulating vulnerable individuals into engaging in inappropriate or harmful behaviour. This risk highlights the importance of educating young people about maintaining privacy and recognising potential warning signs.
3. **Exposure to Inappropriate Content:** Young people can accidentally or intentionally come across inappropriate and harmful content while browsing the internet. This may include violent or graphic material, explicit images, or extremist ideologies. Exposure to such content can negatively impact a young person's mental well-being and values.
4. **Privacy and Data Security:** Sharing personal information online without adequate precautions can put young people at risk of identity theft, fraud, or other forms of exploitation. They may unknowingly share sensitive information, making them vulnerable to cyberattacks and misuse of their data.
5. **Online Scams and Phishing:** Young people may fall victim to various online scams and phishing attempts. Scammers use deceptive tactics to trick individuals into revealing personal information, such as passwords or financial details, which can lead to financial loss or identity theft.

6. **Unhealthy Online Behaviours:** Excessive screen time, addiction to social media, and seeking validation through online platforms can lead to negative impacts on young people's mental and emotional well-being. It is crucial to promote healthy digital habits and a balanced approach to technology use.
7. **Sexting and Non-Consensual Sharing of Content:** The practice of sharing intimate or explicit images or messages (sexting) can lead to severe consequences if the content is distributed without consent. Such actions can result in emotional distress, social stigma, and legal implications.
8. **Cybersecurity Vulnerabilities:** Young people may lack awareness of cybersecurity best practices, such as using strong passwords, updating software, and avoiding suspicious links or downloads. This can expose them to hacking, viruses, or unauthorised access to their devices.
9. **Radicalisation and Online Extremism:** The internet can be a breeding ground for extremist ideologies, and young people may inadvertently or purposefully be exposed to radical content. Understanding and identifying such content is vital in preventing radicalisation and promoting tolerance and inclusivity.

By recognising and addressing these risks in our Online Safety Strategy, we can help to develop comprehensive measures to protect and support young people in their online interactions and experiences. Education, open communication, and fostering responsible digital citizenship are essential components of mitigating these risks effectively.

Our Commitment to Ensuring Online Safety:

We are dedicated to creating a safe online environment for young people. This commitment includes:

i) Regularly reviewing and updating our online safety policies and procedures.
ii) Collaborating with schools, educational institutions, parents, and other stakeholders to promote online safety.
iii) Providing training and support for professionals working with young people to enhance their understanding of online safety issues.
iv) Encouraging the responsible use of digital technology and fostering a culture of digital citizenship and resilience.

Collaborating with Schools and Educational Institutions:

We recognise the vital role that schools and educational institutions play in shaping young minds. By working closely with them, we aim to integrate online safety into the curriculum and provide educators with the resources they need to address online safety effectively.

Engaging with Parents and Guardians:

Parents and guardians are essential partners in safeguarding young people online and yet many carers feel the generation gap with their children when it comes to online behaviour; they may feel out of their depth when discussing the internet and social media. We will signpost, promote and help develop awareness campaigns and workshops to equip parents with the knowledge and skills to support their children's online activities safely.

Parents are encouraged to have conversations from a young age and set rules and agree boundaries:

It's useful to agree on some ground rules together. These will depend on the child's age and what parents feel is right for them, but parents might want to consider:

- the amount of time they can spend online.
- when they can go online
- the websites they can visit or activities they can take part in
- sharing images and videos
- how to treat people online and not post anything they wouldn't say face-to-face.
- deploying parental controls (Remembering that filtering is only part of the solution)
- For more information for parents about setting rule and agreeing boundaries, see the family agreement advice that has been published by CHILDNET (http://www.childnet.com/resources/family-agreement).

If a child plays online games:

- check the age rating before they play
- make sure you know who they're playing with
- talk to them about what information is OK to share with other players
- negotiate the amount of time they spend playing online games.

Appendix 2 contains practical advice for parents from Young Minds, a charity dedicated to making sure every young person gets the mental health support they need, when they need it, no matter what. Parents Helpline 0808 802 5544 Mon-Fri 9.30am-4pm

Building Digital Literacy and Resilience:

Promoting digital literacy is crucial for young people to navigate the online world confidently. We will support initiatives that educate young people on critical thinking, media literacy, and recognising misinformation to build their resilience against online risks.

Reporting and Responding to Online Safety Concerns:

We will identify clear reporting mechanisms for online safety concerns, ensuring that young people and their families can seek help and support when facing challenges online. Prompt and appropriate responses to reported incidents will be a priority.

Appendix 3: Reporting Concerns

Training and Support for Professionals:

Professionals working with young people, including teachers, youth workers, and social workers, will receive specialised training to address online safety issues effectively and provide informed guidance to young people.

Evaluating and Improving the Strategy:

Regular evaluation of the strategy's effectiveness will be conducted, taking into account feedback from stakeholders, data on reported incidents, and emerging trends in online behaviour. This process will allow us to adapt and enhance our approach continuously.

Conclusion:

This Online Safety Strategy represents our commitment to ensuring that young people in our community can enjoy the benefits of the internet safely. By working together with schools,

parents, professionals, and young people themselves, we can create a positive and secure online environment for all.

Appendix 1: Resources and Guidance

Resources List

For parents, carers and young people:

LGfL Digisafe
https://parentsafe.lgfl.net/

Information for parents about keeping children safe online and beyond. Split into sections with useful videos and tips about apps, behaviours and reporting issues.

Thinkuknow
www.thinkuknow.co.uk

Information and advice around keeping children and young people safe online. You can find resources for different age groups, as well as films, Q&As and advice around privacy, bullying, grooming, sexting, selfies and more.

ParentZone
www.parentzone.org.uk

Information for families and schools on issues that are caused or amplified by the internet. Advice covers areas such as social media, apps, a guide on how to talk to your child, digital footprints and more.

Internet Matters
www.internetmatters.org

Not-for-profit organisation helping to keep children safe in the digital world. Comprehensive information on specific issues, advice for parents, controls and how to get further help or report issues.

Kidscape
www.kidscape.org.uk

Equipping young people, parents and professionals with the skills to tackle bullying and address safeguarding issues. Parent Advice Line open Monday-Wednesday from 9.30am-2.30pm.

Phone: 020 7823 5430

Information for parents: http://www.kidscape.org.uk/advice/advice-for-parents-and-carers/cyberbullying-and-digital-safety/

UK Safer Internet Centre
www.saferinternet.org.uk

Provides a range of resources for primary and secondary age ranges, as well as information for parents.

NSPCC
www.nspcc.org.uk

Advice on a range of online issues, including how to talk to your child about online activity, at www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety

Their helpline provides information and advice to anyone worried about something a young person may have experienced online. Open Monday-Friday 8am- 10pm and weekends from 9am-6pm.

Phone: 0808 800 5000

Email: help@nspcc.org.uk

Ditch the Label
www.ditchthelabel.org

Advice and blogs about cyberbullying and updates on the latest social media apps.

CBBC
www.bbc.co.uk/cbbc/findoutmore/stay-safe-facts

Internet information and advice for primary-aged children.

YoungMinds

#Take20

www.youngminds.org.uk/take20

Ideas and suggestions to help parents find 20 minutes to do something together with their child to support confidence, self-esteem and resilience.

Parents Lounge

www.youngminds.org.uk/find-help/for-parents/parents-lounge

Our Parents Helpline experts answer questions on exam stress.

Top Tips

www.youngminds.org.uk/take20/top-tips-for-you-and-your-child

Supporting a child through a time of difficulty or change.

Childline
www.childline.org.uk

If you're under 19 you can confidentially call, chat online or email about any problem big or small.

24/7 helpline: 0800 1111

Chat 1:1 with an online counsellor: www.childline.org.uk/get-support/1-2-1-counsellor-chat

To email: sign up on the website, so you can send your message without needing to use your name or email address, at www.childline.org.uk/registration

The Mix
www.themix.org.uk

If you're under 25 you can talk to The Mix about anything that's troubling you over the phone, email or webchat. You can also use their phone or online counselling service.

Helpline open daily 4-11pm: 0808 808 4994

Email: www.themix.org.uk/get-support/speak-to-ourteam/email-us

Webchat open daily 4-11pm: www.themix.org.uk/getsupport/speak-to-our-team

Counselling service: www.themix.org.uk/get-support/speak-to-our-team/the-mix-counselling-service

Youth Access
www.youthaccess.org.uk

Offers information about advice and counselling services in the UK for young people aged 12-25 years.

Youth Wellbeing Directory
www.annafreud.org/on-my-mind/youth-wellbeing Lists local services for young people's mental health and wellbeing.

MindEd for Families
www.minded.org.uk/families/index.html

MindEd for families is a website where you can hear about other parents' experiences and find clear, helpful guidance on children and young people's mental health and wellbeing.

YoungMinds Crisis Messenger
Provides free, 24/7 text support for young people experiencing a mental health crisis.

Text YM to 85258

Texts are free from EE, O2, Vodafone, 3, Virgin Mobile, BT Mobile, Giff Gaff, Tesco Mobile and Telecom Plus

Resources List

For Teachers, Educators & Professionals

UKCCIS
The UK Council for Child Internet Safety (UKCCIS) was a group of more than 200 organisations drawn from across government, industry, law, academia and charity sectors that work in partnership to help keep children safe online.

UK Council for Child Internet Safety (UKCCIS) - GOV.UK (www.gov.uk)

LGfL safeguarding resources.
Landing page with interactive resource selection. Choose topic by audience, key stage and area of application.

https://lgfl.net/safeguarding/resources

NSPCC
Information and guidance on what you and your organisation can do to protect children from harm. Includes both training and resources.

https://learning.nspcc.org.uk/

National Cyber Security Centre (NCSC)
Advice, resources and opportunities for schools and students interested in cyber security.

https://www.ncsc.gov.uk/section/education-skills/schools

Interactive online security resources for 11–14-year-olds. Lesson plans, assets and practitioner guidance

https://www.ncsc.gov.uk/collection/cyberfirst1114

Award-winning interactive online security resources for 7-11 year olds.
https://www.ncsc.gov.uk/collection/cybersprinters

UK Safer Internet Centre
www.saferinternet.org.uk

Provides a range of resources for primary and secondary age ranges, as well as information for parents.

Their helpline provides support to professionals working with children around online safety issues.

Open Monday-Friday 10am-4pm.

Phone: 0344 381 4772

Email: helpline@saferinternet.org.uk

Appendix 2: Parental Guidance

Advice and information for parents

1. Think about how you guide your family in the real world and how you can do the same in the digital world.

2. Question your own behaviour and what we, as adults, are modelling.

3. Try out the technologies your child enjoys - download some of their music and have a go at games they like. Look at the latest social media trends they are talking about. Download the apps and see how they work or google a guide to it.

4. Talk to your own friends and family about how they manage their children's digital lives. Use some of the resources to make sure you can guide on privacy settings and age restrictions.

5. Bear in mind that policing is not equipping young people with skills for life – guidance and education are essential.

6. Remind older siblings that websites they use may not be suitable for younger brothers and sisters. Be aware of PEGI game ratings – 18 is usually 18 for a good reason.

7. Make digital issues part of ordinary, everyday conversations - talking about subjects like cyberbullying, sexting and gaming and help them understand the consequences.

8. When you're talking about bullying, sex and relationships and other issues, don't forget to include the online aspects.

9. Talk together about "friends". Agree what a true friend is and discuss the problems with people who ask to be your 'friend' online.

10. Talk to your children about whether the issues they face are different online and offline.

11. Don't be afraid to set boundaries and rules

12. Talk to your child about their online reputation and how content (their digital footprint) could remain for years.

13. If your child does tell you about something, try not to overreact as it will discourage them from turning to you again. Remember, they often do not want to see some of the content they might stumble across.

14. There are fantastic resources for parents and carers. Once a month or so, check out the websites in the resources list on the next pages. They will give you up-to-date information about the latest online trends.

Appendix 3: Reporting Concerns

These reporting mechanisms are designed to help individuals, including students, parents, teachers, and members of the public, report various online safety issues, such as cyberbullying, online harassment, harmful content, and illegal activities.

1. Merton's Children and Families Hub: If there is concern that a child is being abused or neglected it should be reported so that the child can be protected. Members of the public should call the police I the first instance if they consider the child is in immediate danger or in a life-threatening situation. For all other less urgent concerns contact the Children and Families Hub (formerly known as the MASH). The trained professionals listen to concerns and make decisions about the next steps to ensure the child's safety and wellbeing.

   Tel: 020 8545 4226 email: candfhub@merton.gov.uk web What You Can Do - Merton Safeguarding Children Partnership (mertonscp.org.uk)

2. Local Police: In cases involving serious online safety issues or illegal activities, individuals can contact their local police force to report the matter. The police will investigate and take appropriate action as necessary.

   https://www.merton.gov.uk/communities-and-neighbourhoods/crime-prevention-and-community-safety/report-crime

   If you or the person you are helping is in immediate danger please contact the police dialling 999

3. CEOP (Child Exploitation and Online Protection) Reporting: CEOP is a law enforcement agency that specialises in protecting children from sexual abuse and exploitation online. They have a dedicated online reporting platform called "CEOP Report" where individuals can report any online behaviour that makes them uncomfortable or raises concerns about child exploitation. The CEOP Report can be accessed through the National Crime Agency website. https://www.ceop.police.uk/ceop-reporting/

4. Childline: a free, private and confidential service where young people can talk about anything, online or on the phone, anytime.
   Tel: 0800 1111 https://www.childline.org.uk/get-support/

5. UK Safer Internet Centre: The UK Safer Internet Centre provides resources and guidance on online safety. https://saferinternet.org.uk/online-issue They also have a reporting tool called "Report Harmful Content," which allows users to report harmful content found on social media platforms, websites, or other online services. The UK Safer Internet Centre also operates the helpline service for professionals and adults with online safety concerns.

   - **Professionals Online Safety Helpline:** Support for professionals working with children and young people, with any online safety issue they may be having. helpline@saferinternet.org.uk Tel: 0344 381 4772
   - **Hotline:** Hotline for reporting and removing sexual images of children online https://www.iwf.org.uk/report/
   - **Report Harmful Content:** https://reportharmfulcontent.com/
   - **Revenge Porn Helpline:** Report intimate images shared online without your consent https://revengepornhelpline.org.uk/

6. Internet Watch Foundation (IWF): The IWF is an organisation dedicated to removing and reporting illegal content on the internet, such as child sexual abuse imagery. They have a reporting tool on their website that allows users to anonymously report any potentially illegal content they come across online. https://www.iwf.org.uk/report/

7. NSPCC (National Society for the Prevention of Cruelty to Children): The NSPCC offers a helpline and an online reporting form for concerns related to child safety, including online safety issues. They provide advice and support to parents and individuals dealing with online safety concerns. https://www.nspcc.org.uk/keeping-children-safe/reporting-abuse/nspcc-helpline/ email: help@NSPCC.org.uk. Tel: 0808 800 5000

8. School Reporting Mechanisms: Schools have their own protocols for reporting and recording online safety concerns. Students and parents can report any incidents or concerns directly to the school's designated safeguarding lead or other appropriate staff members.

9. Social Media Platforms: Major social media platforms like Facebook, Twitter, Instagram, Snapchat, and YouTube have reporting features that allow users to report abusive or harmful content, cyberbullying, or other online safety concerns directly to the platform administrators. For the main platforms please use the links below:

    - **Instagram** https://help.instagram.com/contact/383679321740945
    - **Facebook** https://www.facebook.com/help/1380418588640631
    - **Whatsapp** https://faq.whatsapp.com/414631957536067?helpref=faq_content
    - **Snapchat** https://help.snapchat.com/hc/en-us/requests/new and https://help.snapchat.com/hc/en-us/articles/7012399221652
    - **Twitch** https://safety.twitch.tv/s/article/Filing-a-Report?language=en_US
    - **TikTok** https://support.tiktok.com/en/safety-hc/report-a-problem
    - **YouTube** https://support.google.com/youtube/answer/2802027?hl=en-GB&ref_topic=9387085&sjid=11331615628822182 69-EU

10. Spam, Phishing and scams:

    - Information Commissioners Office (ICO) https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-emails/report-spam-emails/
    - National Cyber Security Centre (NCSC) - If you have received an email which you're not quite sure about, forward it to report@phishing.gov.uk

    If you think you may have been the victim of fraud or cybercrime and incurred a financial loss or have been hacked as a result of responding to a phishing message, you should report this to Action Fraud

It is essential to educate students, parents, and school staff about these reporting mechanisms and encourage them to report any online safety concerns promptly. Reporting plays a crucial role in addressing online safety issues, protecting individuals, and creating a safer digital environment for everyone.