Merton
Safeguarding
Children Board

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

Draft Date	Author	Date Of the Next Review	Lead Manager
May 2014 Revised May 2017 Approved June 2017	P Bailey With D Crabtree	May 2019	MSCB Board Manager

This Online Safety Strategy was developed in consultation with students in years 9 and 10 at Raynes Park High School. Their views and voices have been invaluable in shaping this strategy.

1.1 What is online safety?

Online safety is a term which includes not only the internet but other ways in which young people communicate using social and electronic media; including smart phones, gaming consoles, tablets and computers. It also means ensuring that children and young people are protected from harm and supported to enjoy the full benefits of new and developing technologies without risk to themselves or others.

The aim is to protect young people from the negative consequences of use of electronic media; including bullying, violent extremism, inappropriate sexualised behaviour or exploitation.

Appropriate use of electronic media by service provider staff and professionals is covered by other protocols and procedures with individual services and organisations. Most agencies will already have 'appropriate or acceptable use' policies in place, and all should be encouraged to develop them

1.2 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.

1.3 Consultation

Young People (Youth Inclusion/Participation)
Raynes Park High School
Schools Headteacher Forum (Primary and Secondary)
DSL Forum
MSCB partners

2. Online safety issues and scope of the strategy

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 foot print
- 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 are able to 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

Parents are encouraged to 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.

BRECK'S STORY

Breck Bednar was a 14 year old boy, from Caterham, Surrey who loved technology and online gaming. He was groomed via the internet and murdered on February 17th 2014 by someone he met online. The Breck Foundation is raising the awareness of playing safe whilst using the internet. The foundation has been set up in his memory to help other young people enjoy playing online but to be aware of some simple rules to stay safe.

Be aware Opening files, accepting emails, IM messages, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages

Report it: Tell your parent, or trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied

Educate: Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real friends and family

Communicate: Meeting someone you have met online can be dangerous. Remember online friends are still strangers even if you have been talking to them for a long time. Never meet up with them alone and always speak to a parent or carer beforehand.

Keep Safe: Keep safe by being careful not to give your personal information when you are chatting or posting online. Personal information includes your email address, phone number, password, location

Ignoring age restrictions

Some websites and games use age restrictions and checks to make sure that children don't see unsuitable content. Age restrictions are in place to protect children from accessing or being exposed to material that is inappropriate, disturbing or upsetting: they should not be ignored.

Children must be at least 13 to register on most social networking websites. But there's not a lot standing in the way of children joining at a younger age.[1]

Age limits are there to keep children safe so parents shouldn't feel pressurised into letting younger children join these websites.

Sharing personal information

Privacy controls can limit who can see a child's details, like their name, age and where they live. But when a child connects to someone as a 'friend', that person will have access to your child's personal information.

Some 'free' games might ask children to fill out lots of details before they can play and then illegally rent or sell this data on to others for profit.

Children often sign over rights to their private messages and pictures unknowingly by agreeing to terms and conditions without reading them or comprehending their potential consequences.

Very often, the long established rights of children are not applied online.

Switch off or adjust settings using GPS or location tracking

Lots of apps and social networking sites use software to locate where the user is. Children and young people can also reveal their location by tagging photos, such as on Instagram, or checking in on Facebook or Foursquare.

[1] The General Data Protection Regulation (GDPR) comes into effect in May 2018. Initially this will raise the minimum age to 16 and means that if an organisation seeks consent to process young peoples personal data, then parental consent must be obtained. See https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

This means that people can find out where your child lives, socialises, works or studies.

The strategy covers the following aspects of online safety:

- Inappropriate content
- Cyber-bullying, including sexual bullying
- Online Grooming
- Youth Produced Sexual Images
- Online Reputation
- Privacy
- Self-Harm
- Online Pornography
- Radicalisation

Inappropriate content

What sort of inappropriate content might my child see? What you think is inappropriate material for your child will probably differ from your child's view or that of other parents. It will also depend on your child's age and maturity level. Inappropriate content includes information or images that upset your child, material that's directed at adults, inaccurate information or information that might lead or tempt your child into unlawful or dangerous behaviour. This could be:

- pornographic material
- content containing swearing
- sites that encourage vandalism, crime, terrorism, racism, eating disorders, even suicide
- pictures, videos or games which show images of violence or cruelty to other people or animals
- dangerous advice encouraging eating disorders, self-harm or suicide
- gambling sites
- unmoderated chat rooms – where there's no one supervising the conversation and barring unsuitable comments
- racist, homophobic and other forms of hate speech

It can be difficult to monitor what your child is viewing as they can access this material through any internet enabled device, including mobile ones such as a phone or tablet. Sometimes your child may stumble upon unsuitable sites by accident, through apps they've downloaded to their mobile device or through links they've been sent by friends, chatting to others online, or even through inter-device communication systems such as Bluetooth or Apple's AirDrop.

Online bullying, including sexual bullying.

Online bullying is when someone bullies others using electronic means, this might involve social media and messaging services on the internet, accessed on a mobile phone, tablet or gaming platform. The behaviour is usually repeated. Like any form of bullying, cyber-bullying can be horrible for the children involved and hard for them to talk about. Online bullying can happen via text, email and on social networks and gaming platforms. It can consist of:

- Threats and intimidation
- Trolling
- Harassment and stalking
- Defamation
- Rejection and exclusion
- Identify theft, hacking into social media accounts and impersonation

- Publically posting or sending on personal information about another person
- Manipulation

Online Grooming

Groomers may go to a social network used by young people and pretend to be one of them. They might attempt to gain trust by using fake profile pictures, pretending to have similar interests, offering gifts and saying nice things to the child.

Once they have the child's trust the groomer often steers the conversation towards their sexual experiences, even asking them to send sexual photographs or videos of themselves. Some may try to set up a meeting or even blackmail children by threatening to share the pictures or videos with the child's family and friends.

Online groomers are not always strangers. In many situations they may already have met them through their family or social activities, and use the internet to build rapport with them. Sometimes children don't realise they've been groomed, and think that the person is their boyfriend or girlfriend.

Youth Produced Sexual Images (also known as sexting)

The term 'youth produced sexual images' is used to describe the sending and receiving of sexually explicit photos, messages and video clips, by text, email or posting them on social networking sites. It's increasingly done by young people who send images and messages to their friends, partners, or even strangers they meet online.

Sharing photos and videos on line is part of daily life for many people, enabling them to share their experiences, connect with friends and record their lives. The increase in speed and ease of sharing imagery has brought about concerns about young people producing and sharing sexual images of themselves. This can expose them to risks, particularly if the images are shared further, including embarrassment, bullying and an increased vulnerability to Sexual Exploitation.

If a young person has shared imagery consensually such as when in a romantic relationship or as a joke, or there is no intended malice, it is usually appropriate for the school to manage the incident directly. In contrast, any incident with aggravating factors, for example a young person sharing someone else's imagery without consent and with malicious intent, should generally be referred to the Police.

- **What are the possible consequences of Youth produced sexual images?** Young people may see youth produced sexual images as a harmless activity but taking, sharing or receiving an image can have a long-lasting impact on a child's self-esteem.
- **It may cause emotional distress:** The sharing of inappropriate content can lead to negative comments and bullying and can be very upsetting.
- **It could affect a child's or young person's reputation:** Explicit content can spread very quickly over the internet and affect the child's reputation at school and in their community both now and in the future. It could also affect their education and employment prospects.
- **Youth produced sexual images is illegal:** When children engage in Youth produced sexual images they're creating an indecent image of a person under the age of 18 which, even if they take it themselves, is against the law. Distributing an indecent image of a child – e.g. sending it via text – is also illegal. It's very unlikely that a child would be prosecuted for a first offence, but the police might want to investigate.

Online Reputation

The internet keeps a record of everything we do online – the photos we upload, the comments other people make about us and things we buy. This is our online reputation. It's important children understand how to manage their online reputation and the impacts for them of a negative online reputation. How do I know what sort of online reputation my child has?

Parents are encouraged to find out more about their child's online reputation by taking the following steps:

- **Search for their child online** – use different search engines and check using the child's whole name and other identifying information such as town or nickname. Also search on Google images
- **Look at the kind of information these searches reveal** – are the comments, photos, links appropriate? Do they include private information like their school or address? If your child has a blog, what does it say?
- **If the child is a member of a social networking site, parents should consider joining it themselves and asking to be the child's online connection, or get another trusted adult to do this**. Be aware that some children may have two or more profiles, one they share with their parents, and one they use for talking to their friends put all the information together and see what it says about the child. Does the picture it portrays feel right to you?

Self-Harm

Self-harm is often understood to be a physical response to an emotional pain of some kind, and can be very addictive. Some of the things people do are quite well known, such as cutting, burning or pinching, but there are many ways to hurt yourself, including abusing drugs and alcohol or through an eating disorder.

People who self-harm often say it provides short-term relief to emotional pain. Even though they're aware of the potential damage they may cause, they can find it hard to stop as a result. (Please refer to the MSCB's Self-Harm Protocol)

Online Pornography

As children explore the internet they can sometimes come across sexual content accidentally, and some of what they become exposed to may be unpleasant, hardcore pornography and extreme images. But there are steps you can take to limit their exposure to this kind of inappropriate content. Links
https://www.internetmatters.org/parental-controls/interactive-guide/
http://www.parentsprotect.co.uk/files/Parents%20Pack_Whats%20the%20problem_11Mar2015.pdf

Radicalisation

There's a chance that children may meet people online or visit websites that could lead them to adopting what would be considered to be extreme views, and becoming radicalised. Curiosity could lead a child to seek out these people, or they could befriend a child in order to encourage them to adopt beliefs or persuade them to join groups whose views and actions you as a parent would consider extreme.

How could children become radicalised?

Young people may be vulnerable to a range of risks as they pass through adolescence. They may be exposed to new influences and potentially risky behaviours, influence from

peers, influence from older people or the internet as they may begin to explore ideas and issues around their identity.

There is no single driver of radicalisation, nor is there a single journey to becoming radicalised. The internet creates more opportunities to become radicalised, since it's a worldwide 24/7 medium that allows you to find and meet people who share and will reinforce your opinions. Research tells us that the internet and face-to-face communications work in tandem, with online activity allowing a continuous dialogue to take place. (please see the MSCB's Guidance for Working with Children and Young People who are vulnerable to the messages of Radicalisation and Extremism)

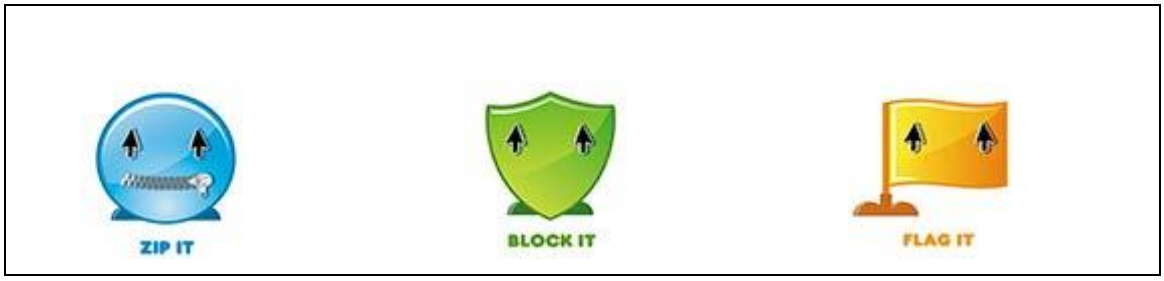
3. Principles of online safety in Merton

A fundamental principle is that the best people to support young people in their online safety are other young people; as they understand the risks and issues, and know what young people are actually doing online. Young people will be helped set up their own structures and resources to help other young people and build resilience

Rather than duplicate existing work, there is a wealth of advice and support available to young people, parents/carers and professionals available nationally. This should be signposted for people in Merton, principally through the MSCB webpages: Staying safe online: http://www.merton.gov.uk/health-social-care/children-family-health-social-care/lscb/online safety.htm

Schools and other young people's organisations will be encouraged and supported to ensure that online safety is at the heart of their efforts to safeguard young people, including identification of those who may be vulnerable. Also, that adults working with children, understand the risks posed by adults or learners who use technology.
This should be both as a part of the Curriculum and PHSE and other pastoral care.

The MSCB supports **Zip It, Block It, Flag It** – the **Click Clever, Click Safe Code**



Launched in 2010 for Safer Internet Day, the code features three simple and memorable actions to remember.

ZIP IT means keeping their personal stuff private and thinking about what they say or do online.

BLOCK IT reminds them to block people who send them nasty messages and not to open any links and attachments they receive by email or through social networks if they're not 100 per cent sure they're safe.

FLAG IT is the final piece of advice. It stands for flagging up to a parent, guardian, teacher or someone in authority anything that upsets them while they are online or if someone asks them to meet up in the real world.

The MSCB also supports **S M A R T** developed by ThinkUKnow.co.uk. SMART stands for:

SAFE - Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

MEETING - Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

ACCEPTING - Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE - Information you find on the internet may not be true, or someone online may be lying about who they are.

TELL - Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

The MSCB also supports 5Rights: http://5rightsframework.com/signatories.html

5Rights takes the existing rights of children and young people (under 18), and articulates them for the digital world. Signatories to the 5Rights framework believe that young people should be supported to access digital technologies creatively, knowledgeably and fearlessly.

The Right to Remove
Every child and young person should have the right to easily edit or delete all content they have created.
"Sometimes people don't think before they act and they can be mean to someone without knowing and wish to take it down later."

The Right to Know
Children and young people have the right to know who is holding or profiting from their information, what their information is being used for and whether it is being copied, sold or traded.
"I never knew that my information is used by other people, I didn't realise how important it is to advertising companies."

The Right Safety and Support
Children and young people should be confident that they will be protected from illegal practices and supported if confronted by troubling or upsetting scenarios online.
"There is too much emphasis on what's illegal and not enough about what is unpleasant or distressing"

The Right Informed and Conscious Use
Children and young people should be empowered to reach into creative places online, but at the same time have the capacity and support to easily disengage.
"It's asking too much to expect us, without support, to behave in ways that challenge the design of sophisticated technologies?"

The Right Digital Literacy
To access the knowledge that the internet can deliver, children and young people need to be taught the skills to use, create and critique digital technologies, and given the tools to negotiate changing social norms.
"*There is a risk of a widening gap between the potential of technology and the reality of our ability to use and understand it."*

Understanding Terms and Conditions
Applications like Instagram, Facebook, Snap Chat etc., have very detailed and confusing terms and conditions. It is important that parents and children understand that when they agree to the terms and conditions of many popular apps children and young people:

- Give up some of their privacy rights
- Information about your can be bought or sold
- The terms and conditions of apps can be changed without notice
- The app could choose to close you account whenever it chooses to[2]

[2] Children's Commissioner for England (2017) Growing Up Digital: A report of the Growing Up Digital Taskforce, p. 9, http://www.childrenscommissioner.gov.uk/sites/default/files/publications/Growing%20Up%20Digital%20Taskforce%20Report%20January%202017_0.pdf

See Appendix A for information and guidance for young people and adults.

4. Priorities

1 Encouraging young people to support other young people and that they are signposted to the best advice.

2 Ensuring parents and carers are signposted to the best advice.

3 Ensuring professionals are signposted to the best advice, particularly existing safeguarding and IT policies.

4 Ensuring schools and all professionals working with young people have support in managing risk in online safety, including how to identify potentially vulnerable young people.

5 Ensuring high quality training is available and taken up by professionals and all appropriate people working with children and young people.

5. Monitoring and accountability – Action Plan

The Merton Safeguarding Children Board will receive a full report on activity annually, and delivery of the strategy will be overseen by the Policy Sub-Group of the Board.

Delivery and guidance in online safety across Merton will be the responsibility of various groups of professionals, particularly in schools and other young people's settings, with the support of, LB Merton Schools ICT Support Team (SMISST), the MSCB:

- Schools IT Managers Forum
- Schools Approved ICT Support Suppliers forum
- Schools Business Manager Forum
- Designated Teachers for Child Protection Meeting

6. Action Plan

Draft Online Safety Implementation Plan			
Outcome	**Next Steps**	**Lead**	**By When**
Ensure Professional Awareness of the Online Safety Strategy Implementation Plan	To develop a Online Safety Briefing Pack for all Safeguarding Leads, Team Managers and Children's workers	PPYP	July 2017
	Disseminate Briefing pack Children's workforce	PPYP	November 2017
	To ensure there is information on online safety on the MSCB webpage	MSCB Business Unit	November 2017
Outcome	**Next Steps**	**Lead**	**By When**
Provide guidance to parents, children and young people on Youth Produced Sexual Images For Primary and Secondary Aged Young People	To Work with Participation Leads and Merton Schools to provide guidance to young people and their families	PPYP Participation Manager Board Manager	March 2018