Kingston and Richmond
Safeguarding Children Partnership

Online Safeguarding Strategy
2020-2022

Contents

Section One

1. Introduction

Individuals often associate online safeguarding with online grooming, online bullying, youth-produced indecent images and sexting. However, there is also a much broader and developing agenda particularly in relation to the growth of social media which may include:

- Exposure to inappropriate or harmful material online e.g. gambling content, pornography or violent content
- “Digital” self-harm
- Problematic internet use (internet “addiction”)
- Exposure to content that promotes worrying or harmful behaviour e.g. suicide, self-harm and eating disorders
- Becoming victims of cybercrime such as hacking, scams/hoaxes, fraud and identity theft
- Becoming a perpetrator of cybercrime such as hacking and piracy
- Radicalisation and extremism online
- Publishing too much personal information online

In line with this, online safeguarding is an increasingly common thread running across a number of related and already embedded areas such as child sexual exploitation (CSE), anti-bullying, antisocial behaviour and the radicalisation of young people among others. If we are to be effective in our approach, it is essential that colleagues across all related agendas work together cohesively to ensure a common and collaborative approach and **ensure the online aspects are appropriately reflected in related risk areas.**

As is apparent, the scope of online safeguarding is significant. However, for the purposes of clarity in the context of this Strategy, **Online Safeguarding** is defined as:

- Promoting the positive and safe use of online technology.
- Reducing the risk of exposure to online content or conduct which risks harm to their health or development.
- A ‘Safeguarding’ incident where online technology is involved.

"Children and young people need to be empowered to keep themselves safe. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." – Dr Tanya Byron, Safer Children in a Digital World (2008)

Educating children and young people (and those adults who support them) on how to recognise the potential risks while online and how to deal with them appropriately should form the core of an effective online safeguarding strategy. Online safeguarding is first and foremost a safeguarding issue and when broken down into its constituent elements and areas of risk, is **fundamentally concerned with behaviours.** It is therefore important that we are not side-tracked into thinking online safeguarding is an ICT issue or that technical measures are the solution to the issues. While ICT has an integral part to play in contributing to the safeguarding of our children and young people, ICT itself is incidental to the issue.

Research from EU Kids Online found

1. The more children use the internet, the more digital skills they gain, and the higher they climb the ‘ladder of online opportunities’ to gain the benefits.
2. Not all internet use results in benefits: the chance of a child gaining the benefits depends on their age, gender and socio-economic status, on how their parents support them, and on the positive content available to them.

3. Children's use, skills and opportunities are also linked to online risks: the more of these, the more risk of harm. As internet use increases, ever greater efforts are needed to prevent risk also increasing.
4. Not all risk results in harm: the chance of a child being upset or harmed by online experiences depends partly on their age, gender and socio-economic status, and also on their resilience and resources to cope with what happens on the internet.
5. Also important is the role played by parents, school and peers, and by national provision for regulation, content provision, cultural values and the education system.

Young people are often perceived as having a greater knowledge and affinity with technology than many adults. However, it does not follow that they also possess the broader wisdom or emotional maturity adults have developed through life experience. It is therefore vital that we encourage them to increase their understanding of the potential hazards technology presents, developing their resilience and how they can help to mitigate the risks to them (and to others) through their behaviour. It is also clear that parents and carers naturally have a fundamental influence on their children's behaviour and as such, have a critical role to play in embedding what is acceptable and unacceptable behaviour online (particularly in relation to the use of social media) and therefore, developing parent/carer awareness and confidence around the online environment is a key priority.

As adults, we will understandably take a perspective of 'responsibility' but it is essential that we retain a 'child-centric' view when approaching the safe use of technology and appreciate how children and young people perceive the risks and the enormous part that technology will play in their lives. Research informs us that issues often go unreported by young people for a variety of factors, including a fear of being held to blame; losing access to the technologies they treasure or simply from embarrassment. If we are to address this issue effectively, we must raise awareness and develop the confidence in utilising the support routes available to children and young people including their own school support mechanisms, CEOP's Report button and ChildLine.

The prevalence of online messaging, social networking and mobile technology effectively means that children can always be 'online'. Their social lives, and therefore their emotional development, are bound up in the use of these technologies. We can no longer adequately consider the safeguarding or wellbeing of our children and young people without considering their relationship to technology - we can no longer seek to support and protect them without addressing the potential risks that the use of these technologies poses.

Members of the children's workforce should have clear standards expected of them in relation to their own use of technologies such as social media, both within and outside the work environment. Equally, professionals must be aware of the potential for online abuse towards them by other users and the options available to them should this occur, as well as the possibility for professionals to behave inappropriately towards other users, which also constitutes abuse.

2. Definition of Online Safeguarding?

'Online Safeguarding', 'e-safeguarding', 'internet safety', 'e-safety', 'digital safeguarding' and 'online safety' are all interchangeable terms used to varying extents. However, regardless of the term used, all should relate to ensuring children and adults using technologies both now and in the future do so safely and responsibly.

3. Key Themes and Issues

The most recent research and statistics have identified the following:

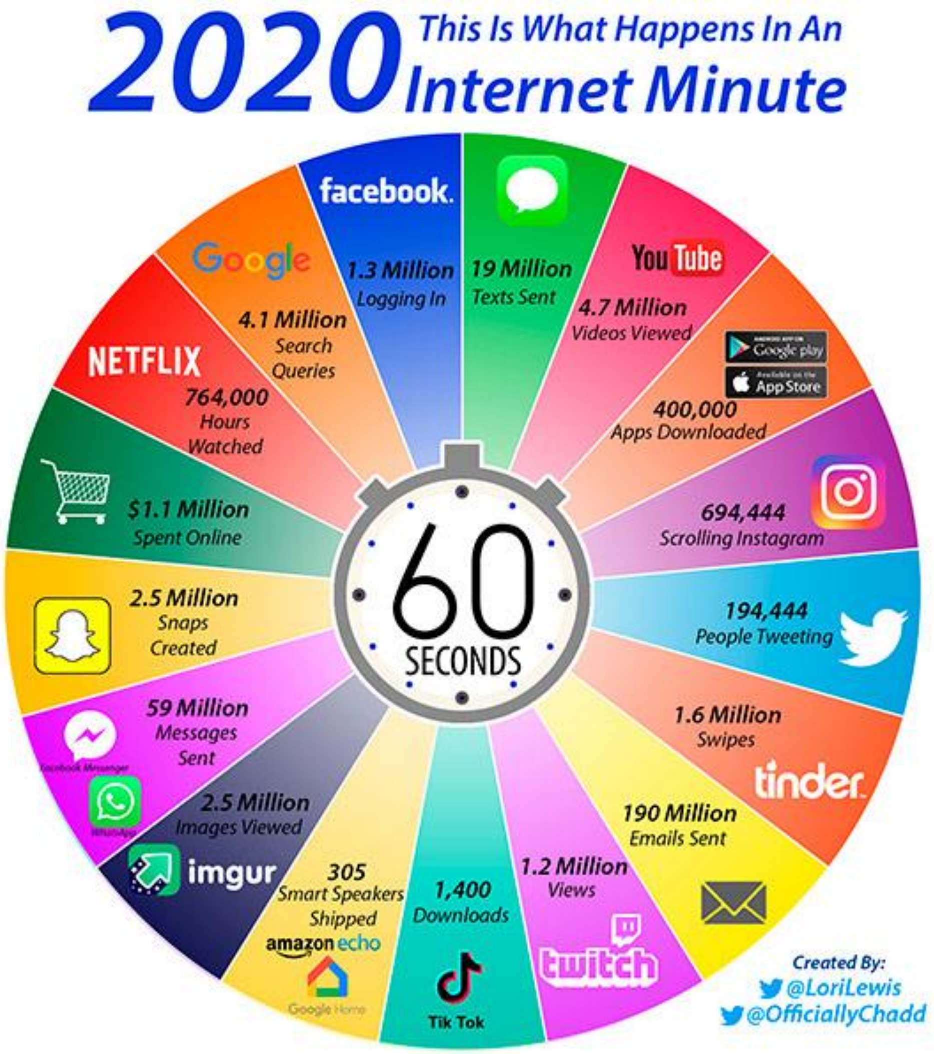
1 in 4 of 8 to 11 year olds and 3 in 4 of 12 to 15 year olds has a social media profile

1 in 3 internet users are children

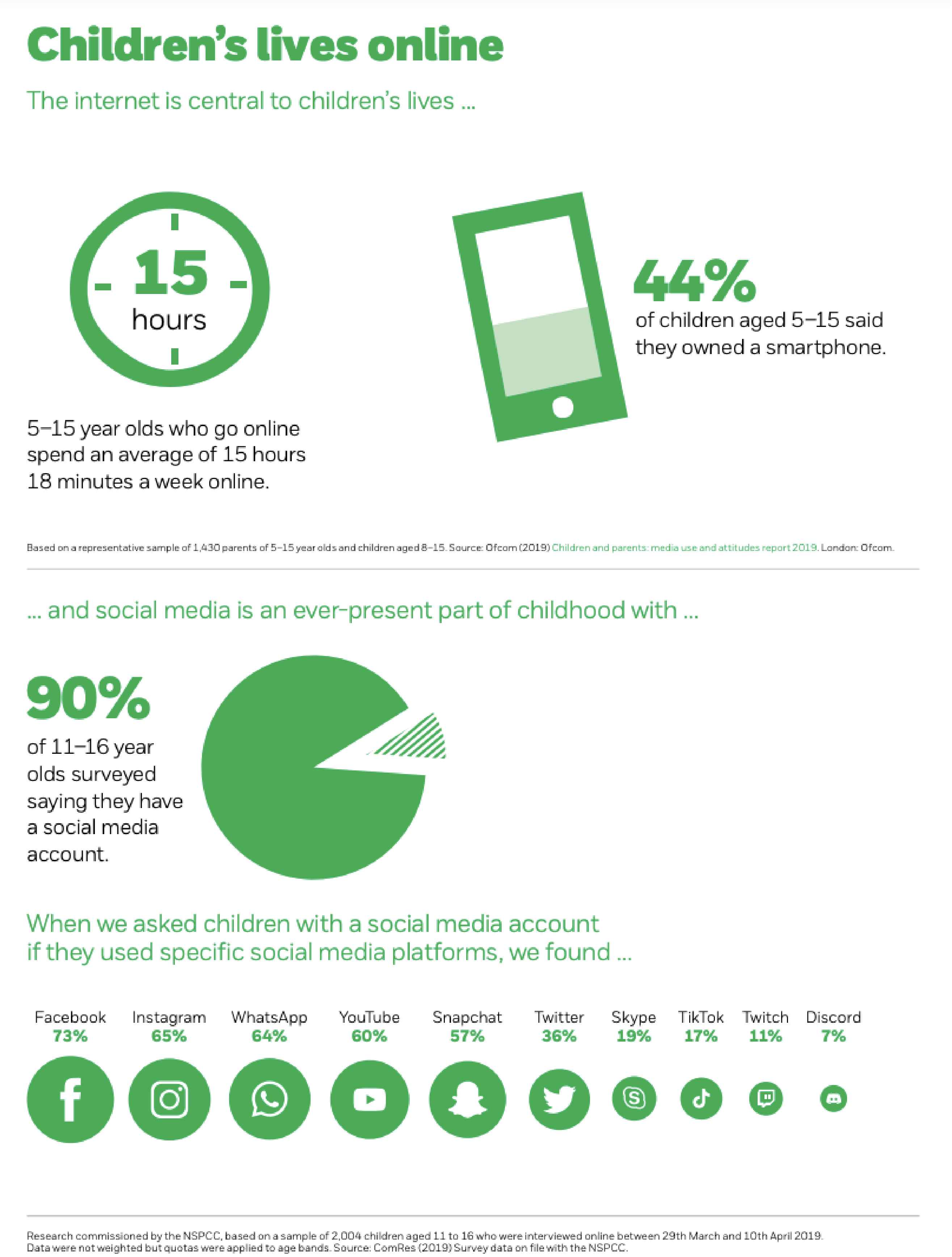
1 in 4 children have experienced something upsetting on a social networking site. Around 1 in 8 young people have been bullied on social media

3 in 4 parents have looked for or received information or advice about how to help their child manage online risks

Almost 1 in 4 young people have come across racist or hate messages online.



NSPCC How Safe Are Our Children Report 2019? Online Abuse:



Children's lives online

The internet is central to children's lives …

15 hours

5–15 year olds who go online spend an average of 15 hours 18 minutes a week online.

44% of children aged 5–15 said they owned a smartphone.

Based on a representative sample of 1,430 parents of 5–15 year olds and children aged 8–15. Source: Ofcom (2019) Children and parents: media use and attitudes report 2019. London: Ofcom.

… and social media is an ever-present part of childhood with …

90% of 11–16 year olds surveyed saying they have a social media account.

When we asked children with a social media account if they used specific social media platforms, we found …

Facebook	Instagram	WhatsApp	YouTube	Snapchat	Twitter	Skype	TikTok	Twitch	Discord
73%	65%	64%	60%	57%	36%	19%	17%	11%	7%

Research commissioned by the NSPCC, based on a sample of 2,004 children aged 11 to 16 who were interviewed online between 29th March and 10th April 2019. Data were not weighted but quotas were applied to age bands. Source: ComRes (2019) Survey data on file with the NSPCC.

3.1 National Information

A report was created by Ofcom using information from their 2019 fieldwork. The findings from the report included the following:

- Half of ten-year-olds now own their own smartphone
- Half of 12-15s say they have seen something hateful about a particular group of people in the last year – up from a third in 2016
- Almost half of parents of 5-15s are concerned about their child seeing content that might encourage them to harm themselves, up from 39% in 2018. There have also been increases in the proportion of parents of 12-15s worried about in-game spending (from 40% to 47%) and game-related bullying (32% vs 39%).

4. What are the Risks?

Keeping Children Safe in Education (KCSIE)[1] places a significant emphasis on Online Safety and firmly embeds the issue within the broader safeguarding agenda. The focus on the responsibilities for schools and colleges are broad and have substantial implications for how governors and proprietors must ensure effective online safety provision is in place. As highlighted in the statutory guidance, "…the breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:"

Emphasising the increasing importance of online safety, KCSIE includes a dedicated section (Annex C), highlighting the three areas (3C's) as:

Content: Many with child as recipient of mass distributed content. For example, being exposed to illegal, inappropriate or harmful material such as pornography

Contact: child as participant in an interactive situation predominantly driven by adults. For example, others who might attempt to groom, radicalise, sexualise or exploit them

Conduct: child as actor in an interaction in which s/he may be initiator. For example, online behaviour that can cause harm to others (Bullying, sharing indecent images of others)

The table below illustrates these categories as a matrix grid identifying examples under headings of Commercial, Aggressive, Sexual and Values. It is important to remember that there is overlap between some of these categories and boundaries are sometimes blurred.

	Commercial	Aggressive	Sexual	Values
Content (Child as recipient)	Advertising Spam Sponsorship Personal Info	Violent, gruesome or hateful content Lifestyle sites	Pornographic / harmful sexual content	Bias Racist Misleading info or advice
Contact (Child as participant)	Tracking Harvesting Personal information	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (Child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating / uploading inappropriate material; e.g. sexting	Providing misleading info and advice e.g. suicide/pro-anorexia

🟩				Health and wellbeing; time spent online

Areas of Risk based on Safer Children in a Digital World: The Report of the Byron Review

As both the technology and the behaviour of individuals change, these risks will also develop. Therefore, if we are to ensure an effective approach, our strategies and policies must be equally robust and regularly reviewed to ensure currency.

Although the grid has been defined in terms of 'child' use, it is relevant to everyone who uses digital and mobile technologies.

1 https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

5. Links with Mental Health

In 2015, the Office for National Statistics found that there is a "clear association" between the amount of time spent online and mental health problems, particularly depression, poor sleep quality and other social and emotional problems. The concept of the **'Fear of Missing Out' (FOMO)** has been robustly linked to higher levels of social media engagement, which has been known to cause distress in the form of anxiety and feelings of inadequacy when not online.

Children, particularly around the time of adolescence, can become obsessed with ideas about themselves and their lifestyle. With smartphone cameras, online filters and image-manipulation techniques, there has been a rise in the popularity of 'selfies'. This has led to concerns about the abundance of idealised images of beauty on social networks and the impact this has on young people's view of their own appearance.

It has been found that young people can access harmful information on the internet or make connections with people online who encourage them to self-harm. For example, some websites imply that unhealthy behaviours, such as anorexia and self-harm, can be normal lifestyle choices. Social networking also provides the opportunity for online groups to form that promote these unhealthy behaviours.

There have been a number of high profile cases involving online bullying and suicides over the past decade and reports of suicide clusters facilitated by social media. It is very easy to find pro-suicide information, such as detailed information on methods, on the internet. Another concern is the risk of 'contagion', where young people are encouraged to take their own lives after witnessing others describing suicidal thoughts or leaving suicide notes on social media. More recently, there have been several reported incidents of young people livestreaming suicides on social media. Research on the internet and self-harm amongst young people found that while young people most often use the internet to find help, there is the risk that the internet can normalise self-harm and discourage young people from talking about their problems and seeking professional help.

Digital self-harm is defined as the "anonymous online posting, sending, or otherwise sharing of hurtful content about oneself." Most commonly, it manifests as threats or targeted messages of hate – the more extreme and rare forms of cyberbullying.

If professionals become aware that a child or young person appears to be accessing online content of this type, this should be raised with relevant others, including the safeguarding lead in their organisation, to ensure this information is shared appropriately and that support can be put in place.

In June 2018, The World Health Organisation (WHO) included "gaming disorder" in its list of mental health conditions in the 11th International Classification of Diseases guidelines. The

WHO characterised a gaming disorder as a "pattern of persistent or recurrent gaming behaviour (‘digital gaming’ or ‘video-gaming’), which may be online (i.e., over the internet) or offline, manifested by: 1) impaired control over gaming (e.g., onset, frequency, intensity, duration, termination, context); 2) increasing priority given to gaming to the extent that gaming takes precedence over other life interests and daily activities; and 3) continuation or escalation of gaming despite the occurrence of negative consequences. The behaviour pattern is of sufficient severity to result in significant impairment in personal, family, social, educational, occupational or other important areas of functioning”.

Similar to other types of addiction, the symptoms for technology addiction can include:

- compulsive checking of text messages
- frequent changing of social networking status and uploading of “selfies”
- a feeling of euphoria while on the Web
- social withdrawal
- loss of interest in activities that don’t involve a computer, phone or gadget
- feelings of restlessness when unable to go online

6. Identifying online abuse:

The following information is aimed to help professionals in considering and recognising possible cases of online abuse.

Online abuse relates to (but is not limited to) the use of technology to manipulate, exploit, coerce or intimidate a child to:

- engage in sexual activity;
- produce sexual material/content;
- look at or watch sexual activities;
- behave in sexually inappropriate ways, thereby grooming a child in preparation for sexual abuse either online or off-line.

It can also involve coordinating, or directing others to coordinate, abuse of children online.

As with other forms of sexual abuse, online abuse can be misunderstood by the child and others as being consensual and/or occurring without the child’s immediate recognition or understanding of abuse or exploitation. In addition, fear of what might happen if they do not comply can be a significant influencing factor.

Financial abuse can be a feature of online abuse. It can involve serious organised crime and can be carried out by either adults or other children.

Online abuse can also include online bullying. This is when a child is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another person using the Internet and/or mobile devices. It is often behaviour between children but could potentially include adults. It is also possible for one victim to be bullied by many perpetrators. In any case of severe bullying, it may be appropriate to consider the behaviour as child abuse by another young person.

The internet can be used to engage children in extremist ideologies. A child or young person may also use the internet to reinforce unhealthy messages such as suicide and eating disorders.

It is important to remember that **no child under the age of 18 can consent to being abused or exploited.**

Many of the signs that a child is being abused are the same no matter how the abuse happens.

A child may be experiencing abuse online if they:

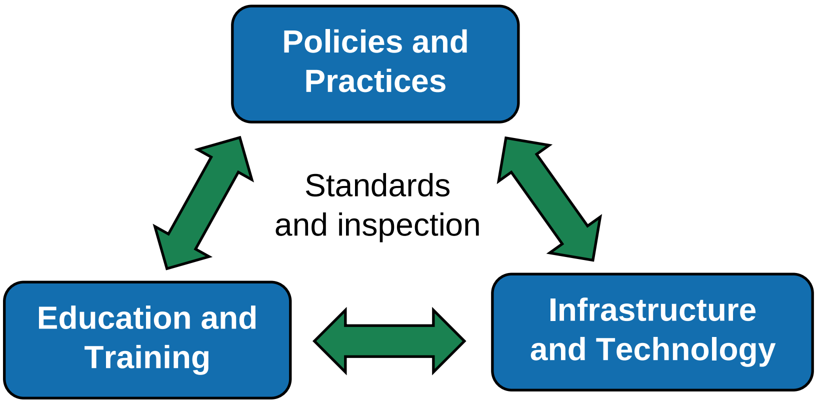
- spend much more or much less time online, texting, gaming or using social media
- are withdrawn, upset or outraged after using the internet or texting
- are secretive about who they're talking to and what they're doing online or on their mobile phone
- have lots of new phone numbers, texts or e-mail addresses on their mobile phone, laptop or tablet.

7. Our approach

The Safeguarding Children Partnership has a statutory duty to safeguard and promote the welfare of children and young people. The KRSCP's objectives are to coordinate what is done by each person or body represented in the Partnership to safeguard and promote the welfare of children and ensure the effectiveness of that work. Traditionally this has referred to the 'real' world but increasingly children are also living in a 'digital' world. We therefore have to adapt our thinking to include new technology and means of communicating and develop approaches to encompass the digital world.

This approach will need to have several strands and to focus on work with children and young people, their parents and carers, and the professionals who work with children and young people. While we must understand the issues and risks posed, we must be careful not to demonise the technology and ensure that these are balanced with the immense opportunities and benefits that new technologies bring.

Managing and mitigating these risks strategically is most appropriately addressed by ensuring we maintain a holistic overview. However, to tackle the issues effectively, we must break them down into practical areas. As such, the framework used for this Strategy is developed from the original and widely-recognised 'PIES Model for limiting e-safety Risk'. This model quantifies online safeguarding into four **inter-related** areas.


Policies and Practices

Standards and inspection

Education and Training

Infrastructure and Technology

Policies and Practices - To support and ensure stakeholders develop and maintain robust and effective policies, practices and procedures to safeguard children and young people against online risks.

Infrastructure and Technology - To identify and promote technologies, tools and infrastructure services that are carefully monitored and which appropriately support online safeguarding priorities for children and young people and related stakeholders.

Education and Training - To promote and support effective learning opportunities for all stakeholders, which recognise and address current and emerging online safeguarding risks for children and young people. The Learning and Development Subgroup will oversee online and face-to-face learning around online safety for partners, children and young people and families. The Learning and Development Subgroup will have, as part of its action plan, themes to follow up around online strategy and learning.

Standards and Inspections - To monitor online safeguarding arrangements and incidents to enable professionals to respond to, manage and support children, young people and families experiencing online concerns. The Quality and Innovation Subgroup will monitor our multi-agency dataset, which will include statistics on allegations made against staff and volunteers, which have a safety element.

8. Online Safeguarding Strategy

While this Strategy provides an overarching framework outlining the scope of online safeguarding and identifies the strategic objectives intended to address the challenges, the operational aspects for how this should be achieved are the focus for the supporting Action Plan. While there has been significant work in recent years, much remains to be done. In addressing the current issues, we must remain vigilant to new and emerging threats and therefore collaborating with, and seeking the views of, Children & Young People will be integral to our success, as will utilising emerging findings and research from organisations (such as IWF, CEOP, NSPCC, Childnet, Parentzone, EU Kids). The Learning and Development Action Plan will therefore have some actions around online safety.

9. Audience

The range of individuals, groups and organisations with a responsibility for safeguarding our children and young people is significant, ranging from parents and carers through to local and national government bodies. As such, this strategy is primarily aimed at (though not limited to) those groups identified below:

- All agencies represented on the Kingston and Richmond Safeguarding Children Partnership
- All education establishments (including maintained schools, independents and academies) and Early Years settings across the boroughs
- 3rd sector organisations, including voluntary, community and faith sectors
- Private and public-sector organisations providing support, guidance and/or training to stakeholders
- All providers delivering services to/for children across Kingston & Richmond
- All private and public sector service providers delivering technical services and points of access utilised by our children and young people

10. Governance

Governance is provided by the Learning and Development Subgroup and scrutiny of progress against the strategic aims and objectives will be undertaken through the regular meetings of this group. .

All partnership members are responsible for implementing and embedding this strategy within their own agency and the KRSCP will hold members to account over this.

11. Summary

It is apparent that online safeguarding is a growing and ever developing area with constantly changing trends and as such, is not a task-and-finish issue nor is it an area where the risks will disappear in the foreseeable future. Equally, the pace at which technology continues to change is enormous and therefore we must also adapt to this change if we are to embrace the challenges and ensure the best possible outcomes for our children and young people.

Section Two

12. Agency and professional responsibilities:

Responsibility of all agencies

No single agency is able to address the complex elements of online safeguarding on its own, largely because a child's and family's needs cannot always be met by a single agency. Effective interventions, whether early help, child in need or child protection depend on professionals developing working relationships that are sympathetic to each others' legal responsibilities, agencies' purpose and procedures, respective roles and agencies' capacities.

All agencies represented on the Kingston and Richmond Safeguarding Children Partnership have a responsibility to contribute to the safeguarding of children across Kingston and Richmond. Roles and responsibilities are clearly defined in both statutory guidance and the KRSCP Procedures and include the following:

- To view the safety and wellbeing of children as paramount.
- To ensure that achieving the best outcomes for the child is the primary focus when working with online abuse.
- To ensure that their workforce understand the significance of all types of abuse against children both in the 'real world' and the 'digital world' and equip their workforce to work effectively in situations where online abuse is a feature. This includes staff understanding the links of online abuse with other types of abuse, particularly child sexual abuse.
- To share relevant information and collaborate with other agencies and work together to ensure accurate assessments and the early identification of needs.
- To harness and develop resources to ensure that interventions are proportionate, effective and delivered sufficiently early so as to reduce the likelihood of any escalation of adversity for the child.
- To ensure that staff attend KRSCP training on all elements of abuse and that the training is embedded in practice.

Responsibility to share information

Information sharing is essential to enable early intervention and preventative work, for safeguarding and promoting welfare and for wider public protection.

It is important that practitioners can share information appropriately as part of their day-to-day practice and do so confidently.

It is important to remember there can be significant consequences to *not* sharing information as there can be to sharing information. You must use your professional judgement to decide whether to share or not, and what information is appropriate to share.

Data protection law reinforces common sense rules of information handling. It is there to ensure personal information is managed in a sensible way.

It helps agencies and organisations to strike a balance between the many benefits of public organisations sharing information, and maintaining and strengthening safeguards and the privacy of the individual.

It also helps agencies and organisations to balance the need to preserve a trusted relationship between practitioner and child and their family with the need to share information to benefit and improve the life chances of the child.

13. Online Safeguarding Incident Flowchart and Guidance notes

Definition of an **Online Safeguarding incident** – "A Safeguarding incident where online technology is involved." Please cross reference with our website documents

Designated Person or Safeguarding Lead

All teams/organisations should have a named person who manages child protection concerns. This Designated Person or Safeguarding Lead will also manage online safeguarding incidents.

Anyone who becomes aware of an online safeguarding incident should record the facts and information as for any other child protection concern. This should be passed on to the Designated Person or Safeguarding Lead. Where a child is deemed to be at risk of significant harm a referral to Children's Social Care must be made.

It is not possible here to list all of the possible offences that can be committed in relation to technology and safeguarding. All staff should therefore consider whether the child/young person or other individual is in **immediate danger** that requires a police response.

Secure evidence

- Take all necessary steps to stop the device from being used – if it is safe and possible so to do.
- Do not delete any evidence e.g. images, messages - Ensure that child is not at risk of further abuse. This might mean removing a device. If able, ensure device is placed in a secure place so evidence cannot be destroyed or the child further abused.
- Do not copy any evidence e.g. images, messages etc as you may be committing an offence.
- Write down what has been seen or sent in accordance with normal child protection procedures.

Member of staff or volunteer is the victim – this may include:

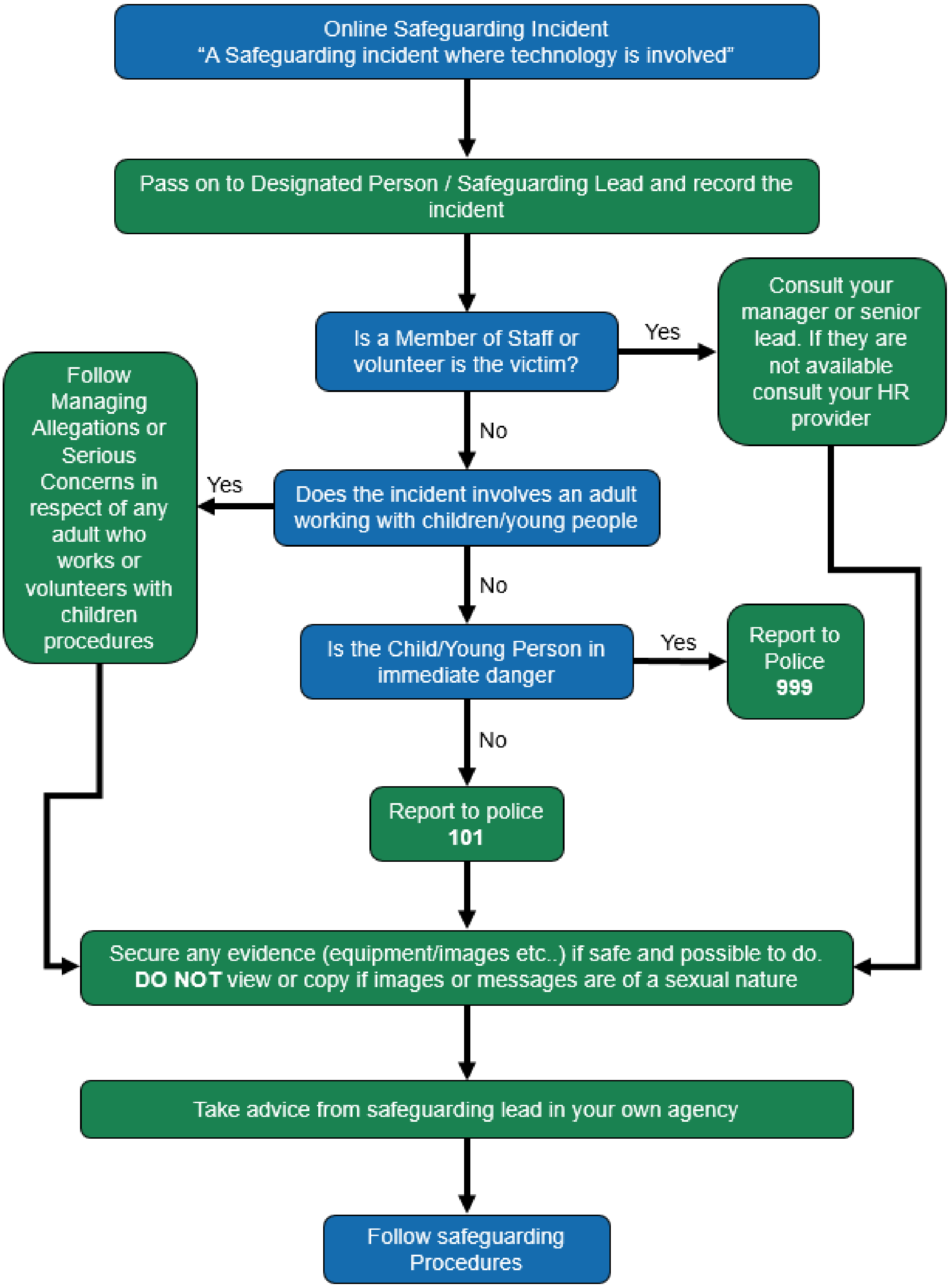
- Cyberbullying – threats, harassment, defamation of character etc.
- Posting of slanderous material
- Creating a bogus social media page

Managing Allegations or Serious Concerns in Respect of Any Adult who Works or Volunteers with Children

The LADO will give further advice as necessary if an online safeguarding incident involves an adult who works or volunteers with children. To contact the LADO for either Kingston or Richmond, please call the Single Point of Access (SPA) team on 020 8547 5008.

The flowchart and guidance refer to various posts within an agency or organisation. Each different agency and organisation will need to determine within their own structure who the relevant officers are.

You come across a Safeguarding concern involving technology…



Online Safeguarding Incident
"A Safeguarding incident where technology is involved"

Pass on to Designated Person / Safeguarding Lead and record the incident

Is a Member of Staff or volunteer is the victim?

Yes: Consult your manager or senior lead. If they are not available consult your HR provider

No: Does the incident involves an adult working with children/young people

Yes: Follow Managing Allegations or Serious Concerns in respect of any adult who works or volunteers with children procedures

No: Is the Child/Young Person in immediate danger

Yes: Report to Police **999**

No: Report to police **101**

Secure any evidence (equipment/images etc..) if safe and possible to do. **DO NOT** view or copy if images or messages are of a sexual nature

Take advice from safeguarding lead in your own agency

Follow safeguarding Procedures

Throughout this process, please ensure that all those involved are supported appropriately

If you think that a child or young person is at risk of serious harm call the **Single Point of Access (SPA)** team IMMEDIATELY.

Phone number: 020 8547 5008

Out of hours emergencies 020 8770 5000

14. Responding to Concerns about the Safety of Children and Young People Online

When there are concerns about the welfare of a child due to activity which has occurred online then the agency should use its usual safeguarding children procedures and good practice to respond to these. In this sense, the context of the abuse / harm occurring online is no different to other situations where there is a concern about a child's welfare.

If there is a concern about actual significant harm or the risk of significant harm to a child arising while online, the agency should immediately activate its own safeguarding children or child protection procedures and make a referral to Children's Social Care - see Making Referrals to Children's Social Care Procedure. Again this is no different to concerns in other situations. If a child or young person is in immediate danger then contact the Police on 999.

When an incident raises concerns both about significant harm and unacceptable use, the paramount consideration should always be the welfare and safety of the child directly involved.

15. Legal Framework

Crimes involving indecent images of children fall under Section 1 of the Protection of Children Act 1978, as amended by Section 45 of the Sexual Offences Act 2003 to extend the definition of children from under 16s to under 18s. It is illegal to take, make, permit to take, distribute, show, possess, possess with intent to distribute, or to advertise indecent photographs or pseudo-photographs of any person below the age of 18. Allowing or encouraging a child to view adult pornography, and/or extreme forms of obscene material is illegal and should warrant further enquiry.

The Serious Crime Act (2015) introduced an offence of sexual communication with a child. This applies to an adult who communicates with a child and the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16 years of age.

The Act also amended the Sex Offences Act 2003 so it is now an offence for a person (A) over the age of 18 to meet intentionally, or to travel with the intention of meeting a child under 16 in any part of the world if they have met or communicated with that child on at least one earlier occasion, and intends to commit a “relevant offence” against that child either at the time of the meeting or on a subsequent occasion. An offence is not committed if (A) reasonably believes the child to be 16 or over.

16. Online Grooming

Online grooming is when someone builds an emotional connection with a child or young person online to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking. This can be a stranger or someone they know such as a friend, a professional or family member, a female or male, adult or peer.

Groomers can use social media sites, instant messaging apps including teen dating apps, or online gaming platforms to connect with a young person or child. They can spend time learning about a young person’s interests from their online profiles and then use this knowledge to help them build up a relationship, or send messages to hundreds of young people and wait to see who responds.

Groomers can easily hide their identity online and pretend to be a child, then become ‘friends’ with children they are targeting. Sexual abuse means a child or young person is being forced or persuaded to take part in sexual activity; this doesn’t have to be physical contact, it can happen online. Increasingly, groomers are sexually exploiting their victims by persuading them to take part in online sexual activity. Child sexual exploitation is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology. Abuse is possible in real time using webcams to provide material for paedophile groups.

Often children and young people don't understand that they have been groomed or that what has happened is abuse.

The impact on a child of online-based sexual abuse and exploitation is similar to that for all sexually abused children. However it has an additional dimension of there being a visual record of the abuse. Online-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse and Child Protection procedures should be followed accordingly.

In addition to grooming a child to physically meet up with them at a location where contact abuse can occur, this may include but is not limited to:

- distribution of indecent photographs/pseudo-photographs (images made by computer graphics or other means, which appear to be a photograph) of children;
- encouraging a child to behave in sexually inappropriate ways or engage in sexual activity;
- the production and distribution of abusive images of children (although these are not confined to the internet);
- where a child or young person is groomed for the purpose of sexual abuse (online or offline);
- where a child is exposed to sexual images and other offensive material via the internet; and
- directing others to, or coordinating, the abuse of children online.

Signs of Online Grooming

The majority of children who are online are not being abused and never will be. The following activities could be perfectly innocent, but it is worth being alert to potential signs:

- Becoming secretive with their phone or computer
- Excessive use of their phone or computer
- Showing aggression if asked about their online use
- Change in the use of sexual language
- Unexplained gifts or cash.

Changes in children's behaviour may also act as indicators and these can include:

- A change in your child's self-esteem and self-confidence
- Withdrawal from family and friends
- Difficulties at school
- An increased level of anxiety
- Sleeping and concentration difficulties
- Becoming excessively concerned with washing and cleanliness.

17. Indecent Images of Children

Contextual Information

There are a number of definitions of ‘Indecent Images of Children (IIOC)’ including ‘youth produced sexual imagery’ or ‘sexting’ but is more appropriately referred to as Self-Generated Indecent Images (SGII). It can be defined as a child (under the age of 18 years) taking an image of themselves or other children under the age of 18 that are indecent or of a sexual nature.

These images are then shared (usually via instant messaging or text messaging) with other young people and/or adults, including with people they may not even know. The content can vary, from images of partial nudity, to sexual images or video. Young people are not always aware that these are in effect images of child sexual abuse and that it is illegal. The widespread use of smart phones has made the practice much more common and the taking of such photographs is often as a result of children and young people taking risks and pushing boundaries as they become more sexually and socially aware.

A factor that appears to drive the creation of self-taken images is children and young people’s natural propensity to take risks and experiment with their developing sexuality. This is linked to, and facilitated by, the global escalation in the use of the internet, multimedia devices and social networking sites.

The reasons why children and young people post sexual images of themselves will vary from child to child. A child would not usually be in possession or be distributing these images because they have an inappropriate sexual interest in children - rather in the majority of cases, it will be as a result of teenage sexual development combined with risk-taking behaviour.

Some self-taken indecent images will be as a result of grooming and facilitation by adult offenders. See Section 4.2, Responses to Adults Involved in Online Sexual Abuse of Children.

Responses to Young People who Post Self-taken Indecent Images

A safeguarding approach is at the heart of any intervention. Parents and carers should be involved at an early stage unless informing them will put the child or young person at risk of harm.

When it is believed young people have viewed abusive images of children, consideration needs to be given to the possibility of the young person being influenced by external experiences (e.g. their own experiences of abuse, prolonged exposure to abusive material by an adult, young person is being groomed etc). Some young people will be at higher risk of developing paraphilic behaviour (a condition in which a person's sexual arousal and gratification depend on fantasising about and engaging in sexual behaviour that is atypical and extreme) as a result of being exposed to abusive images of children. A practitioner who becomes aware of such activity will need to take this seriously, particularly if that young person is living in a household where there are potential victims and may be a child protection issue for the young person concerned.

It is also an offence under the Sexual Offences Act 2003 to cause a child to watch a sexual act.

A person 18 or over (A) commits an offence if:

a) for the purpose of obtaining sexual gratification s/he intentionally causes another person (B) to watch a third person engaging in activity, or to look at an image of any person engaging in an activity.

b) the activity is sexual: and either

  i. B is under 16 and A does not reasonably believe that B is 16 or over, or

  ii. B is under 13

Once an adult/professional becomes aware of any indecent imagery they should not view the imagery unless there is a good and clear reason to do so; any decision to view should be based on professional judgement and clearly recorded.

There should be no downloading or distribution of any images, either internally or externally within the organisation, as this will leave the individuals responsible open to criminal investigation.

The device (including laptops, phones, tablets etc) should be left and not used by anyone, allowing this to be seized as evidence for forensic examination by the police. The details of all persons having access to the computer or device should be made available to allow a clear evidence trail to be established.

The College of Policing has issued a briefing note summarising likely Police action in response to youth produced sexual imagery ('Sexting'). This has made it clear that incidents involving youth produced sexual imagery (where there are no aggravating features) should be treated primarily as a safeguarding issue rather than a criminal offence.

When the police are involved, a criminal justice response against a young person would only be considered proportionate in certain circumstances; the key issue would be if there are any aggravating factors.

First time young offenders should not usually face prosecution for such activities. Instead, an investigation to ensure that the young person is not at any risk and the use of established education programmes should be utilised. The police recommendation is that these cases should be dealt with on a case by case basis, and within a wider safeguarding framework.

Young people who have shared images, or had images shared with or without their consent should be offered appropriate support including help and support with the removal of content (imagery and videos) from devices and social media.

Yoti app supporting the removal of sexual images of children online
Childline and the Internet Watch Foundation have come together to provide a service where children can request the removal of sexual images of themselves which have been shared online. Verification of age and identity is done through the YOTI app. The portal for the removal of images can be found here - https://contentreporting.childline.org.uk

The Criminal Justice and Courts Act (2015) introduced the offence of Revenge Porn where intimate images are shared with the intent to cause distress to the specific victim.

Where young people are voluntarily sending/sharing sexual images or content with one another the police may use the 'outcome 21' recording code to record that a crime has been committed but that it is not considered to be in the public interest to take criminal action against the people involved. This reduces stigma and distress for children and helps to minimise the long term impact of the situation.

Education establishments may also wish to seek advice from the non-statutory guidance

Sexting in schools and colleges: Responding to incidents and safeguarding young people.

Referral and Strategy Discussion

An immediate referral to the police and Children's Social Care should be made if any of these are present (please note this list is not exhaustive):

- The incident involves an adult;
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example owing to special educational needs or disability);
- What is known about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent;
- The imagery involves sexual acts and any child in the imagery is under 18.
- A more slow time referral can be completed (within 24 hours) if it appears the image is between children of a similar age and coercion has not occurred. For example they are in a girlfriend/boyfriend type relationship. This is still an offence and safeguarding advice would be required. The police would not look to criminalise a child in these circumstances but appropriate intervention might be required in co-ordination with partner agencies.
- The child or young person is at immediate risk of harm owing to the sharing of the imagery; this may include arranging offline meetings.

The referral should be made on the same day as a matter of urgency. You should also contact your agency's safeguarding lead.

Where there are concerns that a child may be or is likely to suffer significant harm, Children's Social Care will convene a strategy discussion/meeting involving, health, police and other relevant agencies.

Due to the nature of this type of abuse and the possibility of the destruction of evidence, the referrer should first discuss their concerns with the police and Children's Social Care before raising the matter with the family. This will enable a joint decision to be made about informing the family and ensuring that the child's welfare is safeguarded.

The strategy discussion/meeting will consider:

- The safety of all children within the household, including children in the extended family or social networks with whom the alleged abuser has contact with;
- The safety of the children shown in the abusive images;
- Whether the police will proceed with a criminal investigation
    - the conduct and timing of the investigation

It is worth noting that an investigation does not always conclude with a prosecution.

Responses to Adults Involved in Online Sexual Abuse of Children

As noted earlier, some self-taken indecent images will be as a result of grooming and facilitation by adult offenders. Social networking tools are also often used by perpetrators as an easy way to access children and young people for sexual abuse. The primary purpose of police involvement in these cases should be to ensure that the potential contact with adult exploiters is properly explored. As per police guidance, the focus of investigations should not be on the behaviour of children who have been the victims of abuse or exploitation but on the adult offenders who 'coerce, exploit, and abuse children and young people'.

Adults who have made/taken, downloaded or distributed abusive images of children, have committed an offence under the Sexual Offences Act 2003 and a referral to the police is always required. If the alleged abuser lives in a household with children/young people or comes into contact with children/young people through their personal, work or voluntary activities a referral to Social Care will also be required.

If the alleged abuser works with or volunteers with children or is a foster carer, please refer to the Managing Allegations or Serious Concerns in Respect of any Adult who Works or Volunteers with Children Procedure.

When adults are found in possession of indecent images, partners, colleagues and friends often find it very difficult to believe and may require support.

Information should not be discussed or disclosed to any other individual, including the alleged abuser, their partner or children as it is important there is no opportunity given to the alleged abuser to destroy any evidence that may lead to the identification of victims or be of use in any criminal proceedings. There may be occasions when it is necessary to take action before any strategy meeting has taken place because the risk is time-bound and needs urgent action. Similarly, it may occasionally be necessary to make an arrest without disclosing outside of the police service to ensure offenders are not alerted.

A Strategy Discussion/Meeting should be held on arrest to consider the risk to any children with whom the alleged abuser comes in to contact both in their personal life and through work or voluntary activities. If the images include abusive images of children known to the alleged abuser including his/her own children, an urgent strategy discussion must be held on the same day with a view to commencing a Section 47 Enquiry.

Where the alleged abuser is in a position of trust, either through their work or voluntary activities, a separate strategy meeting chaired by the Local Authority Designated Officer (LADO) will need to be convened within 5 working days. Please see Managing Allegations or Serious concerns in Respect of any Adult who Works or Volunteers with Children Procedure.

All strategy discussions/meetings will need to consider whether the threshold has been met for holding a Section 47 enquiry, and consider if an Initial Child Protection Conference is required. A strategy discussion/meeting may also look at appropriate multi-agency interventions early in the process and seek to minimise risk. In most cases a strategy meeting rather than a discussion is likely to be needed.

The strategy discussion/meeting will need to include the police (who are likely to take the lead in any subsequent enquiries related to criminal proceedings), Social Care and relevant health professionals. The strategy discussion/meeting will consider:

- The safety of all children within the household, including children in the extended family or social networks with whom the alleged abuser has contact with;
- The safety of the children shown in the abusive images;
- When the alleged abuser and their partner will be informed about the investigation, taking into account the time needed by Police to gain and exercise a warrant to seize any electronic equipment;
- Whether the police will proceed with a criminal investigation;
    - the conduct and timing of the investigation

it is worth noting that an investigation does not always conclude with a prosecution.

In the case of staff, volunteers and carers, the LADO discussion will also include:

- Any contact with children or young people through the course of the alleged abusers work or voluntary activities;
- Whether any action should be taken by the employer or agency.

The police and Social Care will conduct a joint investigation. The police investigation is likely to be lengthy, as time is needed to analyse the results of any seized equipment and it is likely that the results of this will not be known within the 45 working days timescale for completing the single assessment. However some key factors can help determine the likelihood of significant harm at an early stage, including:

- previous history (known to Social Care for abuse or neglect)
- previous contact abuse of children;
- images of own children;
- assessment of partner's capacity to protect, indicating that children's safety is likely to be compromised;
- absence of cooperation;
- understanding of risk factors associated with sexual abuse
- known criminal lifestyle.

If any of these risk factors are present, the strategy meeting must consider if the alleged abuser should be asked to leave the home during the assessment and if not, how the risks will be managed. Often this will include the need to devise a written/working agreement to cover matters such as supervision of contact, intimate care of children, entry to children's rooms, sleep-overs etc. Safeguards need to be put into place at the start of any work until a conclusion can be reached about the child/children's safety. Measures such as this are not sustainable in the long term and should be reviewed regularly; this would include the need for a child protection conference.

The use of digital media is not limited by local or national borders. Those undertaking an investigation must always consider the possibility of notifying agencies in other areas (or countries) of their concerns about a child or about an alleged perpetrator.

Social Care Risk Assessment of Individuals Viewing Abusive Images of Children

Social Care involvement is usually (but not always) initiated following notification from the police about a criminal investigation with an individual caught in possession of indecent images of children (IIOC). Individuals who view these images do so as they have a sexual interest in children and have acted on this interest by looking at children being abused. Some individuals will go on to abuse children and others will not. However, careful and holistic assessment is required.

In order to risk assess, the following questions listed below will need to be collated from either the police enquiry or Social Care enquiries and should formulate part of, and not replace, the single assessment process:

- What is known about the nature of images (Category A-C) age, gender of children?
- What is the source of images, e.g. commercial site, home-made images, chat rooms, is there evidence of trading?
- Was any additional material seized at the property (in addition to the hard drive) e.g. disks/DVDs, videos, printed images, written material, were they hidden?
- What other technology was present in the house, e.g. webcam, digital camera, video camera, games consoles?
- If children do not live within the household, was there evidence of toys or other child centred objects?
- Is there any indication children were present while material was being viewed or other material featuring children known to the alleged abuser?
- Is there evidence of heavy alcohol use/drug use/distributing drugs e.g. cannabis?
- Was adult pornography present as well (though adult pornography may or may not be illegal, it is still likely to be relevant to the assessment)?

- How does the alleged abuser initially present her/himself, explore background history, significant life events, previous partners and children including any contact arrangements?
- Any known previous professional involvement? Is there a history of domestic violence or abuse? Is there any prior criminal history?
- How does the non-offending parent initially react to the situation? Is the non-abusing parent less or more able to protect? Does the couple's relationship increase or lower risk?
- How do children in the household present themselves and/or react to the situation (bearing in mind age and development)? Consider each child individually. Do their own circumstances increase or decrease their vulnerability?
- Who are the safer group of significant people to the children, e.g. grandparents? Do agencies involved with the family have any concerns?
- Any initial indicators of abuse/neglect? Do parenting styles increase or lower risk? What are the protective factors in the situation?
- What are the children's daily routines particularly with regard to intimate care and bedtime routines?
- What social and community support is available to the family? Are they socially isolated? What contact does the alleged abuser have with children and young people beyond the immediate family? Consider contact with extended family and community
- Does the alleged abuser come into contact with children or young people through their work or voluntary services?

18. Online Bullying

Online abuse may also include online bullying, sometimes known as cyber-bullying. This is when a child is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child using the internet and digital technology including mobile devices. It is essentially behaviour between children, although it is possible for one victim to be bullied by many perpetrators. In any case of severe bullying (including online bullying) it may be appropriate to consider the behaviour as child abuse by another young person.

Children can engage in, or be a target of, online bullying via text/instant messaging or social networking tools such as WhatsApp and Snapchat and can include being tormented, harassed, humiliated and embarrassed by other users. This form of bullying is a growing problem in schools and other educational settings (see Cyber Bullying Advice for Head Teachers and School Staff, DfE, and Childnet Cyberbullying: understand, prevent and respond guidance for schools and practical PSHE toolkit.).

Online bullying – similar to bullying in the 'real / physical world' – should be taken seriously by any practitioner who becomes aware of it as this can lead to serious physical harm, for example if victims turn to self-harm or suicide. All instances of online bullying should be recorded and responded to sensitively and in line with existing anti-bullying policies and procedures and if necessary concerns should be reported to the police.

The Department for Education has also issued guidance for parents and carers on cyberbullying (see Advice for Parents and Carers on cyberbullying, DfE).

19. Online Extremism and Radicalisation

Radical and extremist groups use social media as a way of attracting and drawing in children and young people to their particular cause; this is similar to the grooming processes and exploits the same vulnerabilities. The groups concerned include those linked to extreme Islamist, or far right/neo-Nazi ideologies, various paramilitary groups, extremist animal rights groups and others who justify political, religious, sexist or racist violence.

A common feature of radicalisation is that the child or young person does not recognise the exploitative nature of what is happening and does not see themselves as a victim of grooming or exploitation.

Where there are concerns in relation to a child's exposure to extremist materials, a number of agencies including the child's school may be able to provide advice and support. In accordance with the government's Prevent Duty, schools and statutory agencies are required to identify a PREVENT lead who is the lead for safeguarding in relation to protecting individuals from radicalisation and involvement in terrorism.

Suspected online terrorist material can be reported through www.gov.uk/report-terrorism. Though reports can be made anonymously, practitioners should not do so as they must follow the procedures for professionals.

If a child or adult is recognised as being at risk to radicalisation a referral can be made to CHANNEL panel.

Content of concern can also be reported directly to social media platforms – see Safety features on Social Networks.

20. Live Streaming and Geo-Location

Live streaming is the broadcasting of a live video recording from internet-connected devices such as phones, tablets or games consoles. The recorded footage is unedited and is viewed in real time by users similar to live TV through services such as Twitch, Facebook, YouTube, Instagram, Periscope and Tik Tok, which are difficult to moderate. It is possible for children and young people to view content that is inappropriate for their age even if they did not intend to watch that type of video.

Some live streaming services allows viewers to comment on a live video as it is being broadcast. Adult offenders will sometimes use tricks and dares to coerce young people into performing acts that involve nudity on camera. Younger children can be particularly susceptible to these tactics as it can be difficult for them to spot manipulative behaviour in others and stand up to pressure.

It is important to remind young people that if someone asks them to remove clothing or do anything sexual, to stop and tell someone. No matter who instigated the conversation or what's been said, it is never the young person's fault. It can then be posted and passed online very quickly. Encourage them to tell an adult and report to CEOP.

There are many location-based apps available for devices and these may be useful for digital assistants such as Alexa, Cortana, Google Now and Google Maps. However when geo-location is shared by services like Instagram or Snapchat, posts and photos are tagged to a location on a map. This can be misused including by sexual predators who may use this information to see the places a young person visits.

Appendix 1 – Learning & Development Sub Group Terms of Reference

Kingston and Richmond
Safeguarding Children Partnership

Kingston & Richmond Safeguarding Children Partnership
Learning & Development subgroup Sub Group
Terms of Reference

Purpose:

The Learning and Development Sub Group is responsible for the identification, planning, delivery and evaluation of training to ensure all those coming into contact/working with children in the boroughs of Richmond upon Thames and Kingston upon Thames are competent and up to date with current legalisation and procedures to help them safeguard and promote the welfare of children effectively.

The sub group ensures that policies and procedures are in place relating to training people who work with children and young people or in services affecting the safety and welfare of children. It oversees the provision and evaluation of safeguarding training across the children's workforce in both boroughs. It also ensures that the learning and development activity takes account of developments in national and regional policy and practice, as well as relevant research, and provides advice to agencies on their in-house safeguarding training.

Roles and responsibilities:

- To develop and implement a strategy for multi-agency safeguarding training.
- To commission and implement a suitable multi-agency training programme for the partnership.
- To ensure the Kingston and Richmond Safeguarding Children Partnership's training programme is developed within the context of current local, regional and national policies, research and practice developments.
- To ensure that training reflects an understanding of the rights of the child and is informed by an active respect for diversity and a commitment to ensuring equality of opportunity.
- To manage the identification of training needs and use this information in the planning and commissioning of the KRSCP training programme to ensure needs are met.
- To monitor access to and take up of single and inter-agency safeguarding training to ensure that local needs are being met across all sectors, including the voluntary and community sector.

- To ensure that both single and inter-agency training is delivered to a consistently high standard.
- To monitor and evaluate the effectiveness and impact of the KRSCP training programme to inform future developments and improvement.
- To promote the training programme and encourage agencies / teams to access both single agency and multi-agency training opportunities.
- To coordinate and ensure the effectiveness of online safeguarding work across all member agencies on behalf of Kingston & Richmond Safeguarding Children Partnership and effectively promote and safeguard the welfare of children and young people in a digital world
- To offer opportunities to embed learning and change practice
- To maintain strong links with the Quality and Innovation and Serious Case Review Sub Groups to ensure that learning from these groups and themes identified are incorporated into the KRSCP training programme.
- To monitor the training budgets for KRSCP and provide reports to the KRSCP main Boards as required.

Governance arrangements:

The Learning and Development Sub Group is chaired by Suzanne Parrott, Head teacher, AFC Virtual School and is coordinated by Daksha Mistry, Learning & Development Manager, and KRSCP.

- Sub Group meetings will take place four times per year.
- Sub group members are expected to attend every meeting. Where there is a legitimate reason for nonattendance an apology must be sent and a representative nominated to attend. Attendance at Sub Group meetings will be monitored and lack of representation from agencies will be highlighted.
- Meeting agendas will be circulated at least five working days before the meeting. Minutes will be distributed to Sub Group members after the meeting.
- The Sub Group Chair will report quarterly on activity and outcomes achieved by the sub group to the Kingston and Richmond main Boards. The sub group chair will attend the meeting of sub group chairs facilitated by the Chair of KRSCP.

Sub Group members’ responsibilities:

- To attend sub-group meetings four times a year and at more regular intervals, where necessary.
- To take an active role in the delivery, monitoring and evaluation of both single agency and multi-agency training

- To ensure all managers and staff across all sections of the partnership are aware of training and development opportunities, including KRSCP training, and to promote the relevance of ongoing professional development in the work of safeguarding and protecting children.
- To develop opportunities to embed learning from audits, Child Practice Safeguarding Reviews and LLRs
- To ensure the training delivered by KRSCP or other training providers is consistent with the KRSCP training strategy, legal frameworks, current safeguarding policies & procedures, and the wider safeguarding agenda.
- To provide a Learning and Development Annual Report to the KRSCP Senior Leadership Group.
- To raise awareness and support within your own setting and sector of the multi-agency training and learning opportunities being offered by KRSCP

Appendix 2: Resources & Web links

National Resources

- Child Safety Online – a Practical Guide for Parents and Carers whose Children are using Social Media
- **Internet Watch Foundation** (www.iwf.org.uk/) – the UK hotline for reporting criminal online content
- **Child Exploitation and Online Protection Agency (CEOP)** (ceop.police.uk/) - protecting children from sexual abuse and making the internet a safer place
- **Think You Know** (www.thinkuknow.co.uk/) – Internet, mobile phone and technology safety for children and young people
- **Stop it Now** (www.stopitnow.org.uk/) - confidential helpline for anyone who has concerns that someone they know may be abusing a child. Also offers support and advice to those are concerned about their own thoughts and behaviours towards children. Telephone 0808 1000 900.
- **Lucy Faithful Foundation** (www.lucyfaithfull.org.uk/) - expertise in this area and can conduct assessment as part of a service level agreement.
- **NSPCC** (www.nspcc.org.uk/)
- Sexting in schools and colleges: Responding to incidents and safeguarding young people (2016)
- **Childnet International** (www.childnet.com/) – includes the resources from KnowITAll (www.childnet.com/resources/kia/)
- **UK Safer Internet centre** (www.saferinternet.org.uk/)
- **Professionals Online Safety Helpline** (www.saferinternet.org.uk/professionals-online-safety-helpline) - Supporting all professionals working with children and young people including teachers, social workers, doctors, police, coaches, foster carers, youth workers with concerns regarding online safety issues. Telephone 0344 381 4772
- **Kidsmart** (www.kidsmart.org.uk/) - internet safety website
- **Pan-European Game Information service** (www.pegi.info) – A resource available to professionals working with children and young people, parents or carers to help determine the correct age of games
- **The Parent Zone** (www.theparentzone.co.uk/) - parenting in the digital age

Appendix 3. Further Information and Legislation

Coram Children's Legal Centre – LawStuff is run by Coram Children's Legal Centre and gives free legal information to young people on a range of different issues. See Children's rights in the digital world in particular.

See Sexting Advice for Parents (NSPCC), UK Safer Internet website and CEOP, thinkUknow website and Childnet Advice on Sexting.

Behaviour that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation. There are a number of pieces of legislation that may apply including:

Computer Misuse Act 1990 – This Act makes it an offence to:

- Erase or amend data or programs without authority; Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities; Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998 – This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Act states that person data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000 – The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003 – Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988 - It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000 – It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security; Ensure the effective operation of the system;
- Monitoring but not recording is also permissible in order to:
  - Ascertain whether the communication is business or personal;
  - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Telecommunications Act 1984 – It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice and Public Order Act 1994 – This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Criminal Justice and Courts Act (2015) – has created a new statutory offence of 'disclosing private sexual photographs and films with intent to cause distress' which seeks to address the problem of 'revenge porn'. The rise of incidents of intimate images being posted online without consent has become a serious concern due to the increasingly prevalent culture of 'sexting' and the technological advances which have made it easy to reproduce and distribute photographs and videos online. This has become a particular problem amongst young adults and teenagers. Under s.33 it is offence to disclose a private sexual photograph or film if the disclosure is made without consent and with the intention of causing distress

Racial and Religious Hatred Act 2006 – This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997 – A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Public Order Act 1986 – This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964 – Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

The Education and Inspections Act 2006 – Empowers school Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Protection of Children Act 1978 – It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003 – The offence of grooming is committed if you are over 18 and have communicated with a child under 16 on one occasion (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Serious Crime Act 2015 – The Act introduces a new offence of sexual communication with a child. This would criminalise an adult who communicates with a child for the purpose of obtaining sexual gratification, where the communication is sexual or if it is intended to elicit from the child a communication which is sexual and the adult reasonably believes the child to be under 16.

Appendix 4 - Keeping Children Safe in Education 2020

Annex C: Online safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views
- Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Education

Opportunities to teach safeguarding, including online, are discussed at paragraph 80-82. Resources that could support schools and colleges include:

- **Be Internet Legends** developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- **DisrespectNobody** is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- **Education for a connected world framework** from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety
- **PSHE association** provides guidance to schools on developing their PSHE curriculum
- **Teaching online safety in school** is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- **Thinkuknow** is the National Crime Agency/CEOPs education programme with age specific resources
- **UK Safer Internet Centre** developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Filters and Monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the above risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.[3]

The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

[3] The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance for Further Education Institutions

Reviewing online safety

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCCIS have recently published online safety in schools and colleges: Questions for the governing board

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	What it does/provides
Think'u'know	NCA CEOPs advice on online safety
Disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
SWGfL	Includes a template for setting out online safety policies

Internet Matters	Help for parents on how to keep their children safe online
Parent zone	Help for parents on how to keep their children safe online
Childnet Cyberbullying	Guidance for schools on cyberbullying
PSHE association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
Educate Against Hate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
The use of social media for online radicalisation	A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
Net-Aware	NSPCC advice for parents
Common Sense Media	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
LGfL	Advice and resources from the London Grid for Learning