Wandsworth Safeguarding Children Board

Online Safety Strategy

Safeguarding children and young people in a digital world

Version Control:

<table>
<thead>
<tr>
<th>Author</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSCB e-Safety working group</td>
<td>1.0</td>
<td>16/02/2008</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Agreed</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSCB Executive</td>
<td>15/09/2014</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contributors</th>
<th>Revision</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSCB e-Safety Task &amp; Finish group</td>
<td>2.0</td>
<td>03/04/2014</td>
</tr>
<tr>
<td>WSCB Online Safety Task &amp; Finish Group</td>
<td>2.1</td>
<td>28/08/2014</td>
</tr>
<tr>
<td>Updated KCSIE 2018 and Data Protection Act 2018.</td>
<td>2.2</td>
<td>22/12/2017</td>
</tr>
<tr>
<td></td>
<td>2.3</td>
<td>08/01/2018</td>
</tr>
<tr>
<td></td>
<td>2.4</td>
<td>06/02/2018</td>
</tr>
<tr>
<td></td>
<td>2.5</td>
<td>21/08/2018</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File location</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.wscb.org.uk">www.wscb.org.uk</a></td>
<td></td>
</tr>
</tbody>
</table>
## Contents

1. Audience ...................................................... 3
2. Introduction .................................................. 4
3. The issues and risks ........................................ 6
   (a) Grooming 
   (b) Cyber-bullying
   (c) Online pornography
   (d) Radicalisation (Prevent)
   (e) Inappropriate content
   (f) Youth-produced sexual imagery (sexting)
   (g) Self-harm
   (h) Online reputation
   (i) Privacy and identity theft
4. How we will tackle Online Safety issues .................. 13
5. Local governance – Online Safety in Wandsworth ....... 14
6. Roles and responsibilities ................................... 15
7. WSCB Strategic Priorities .................................... 16
8. Monitoring and evaluation ................................... 16
9. Appendix 1 – Glossary ....................................... 17
10. Appendix 2 - What do we do if? ......................... 18
11. Appendix 3 - Legal framework ......................... 20
12. Appendix 4 – LGfL School Online Safety Policy template 23
13. Appendix 5 – Cyber-bullying ......................... 44
14. Appendix 6 – Online Safety contacts, links and further information 48
1. Audience

This document is to be used for information, advice and guidance by the following:

- All partner agencies of the WSCB
- Schools and colleges
- Youth clubs
- Other settings for children, young people and families
- Libraries
- Commercial enterprises that provide Internet for public use i.e. Internet cafés
- Voluntary, community and faith groups
2. Introduction

“For better and for worse, digital technology is now an irreversible fact of our lives. In a digital world, our dual challenge is how to mitigate the harms while maximising the benefits of the internet for every child.” UNICEF Executive Director Anthony Lake (Dec 2017).

Wandsworth Safeguarding Children Board (WSCB) believes that we must teach children to be outstanding digital citizens, not only to ensure their safety, but also to enable them to improve their emotional health and well-being, and their enjoyment of the world. Online Safety is about balancing opportunities with risks and we believe as firmly in maximising opportunities as in minimising risks.

WSCB also believes that in order to maximise the opportunities within this environment, whilst concurrently minimising the risks, we must encourage children and young people to develop as responsible online citizens. Such citizens will recognise their responsibility to keep themselves and their peers safe online, but they will also recognise the responsibility they have to present themselves as positive role models. It is only through the development of a sense of online responsibility that we can ensure the safety and well-being of today’s children and young people.

It is acknowledged and agreed by the Wandsworth Safeguarding Children Board (WSCB) that an online safety concern is not just an ICT issue but, fundamentally, a safeguarding and child protection concern, which needs to be acted upon accordingly. Likewise, responsibility for online safety should not always be delegated to technical colleagues alone, or those with a responsibility for ICT, but must be firmly embedded within safeguarding policies and practices.

For many young people, the online world, with all its various forms, is very much their reality. The Internet offers them unprecedented opportunities to communicate, create, discover and be entertained in a virtual environment. Unfortunately, it also offers others who seek to abuse children and young people with the opportunity for unprecedented contact and access to them.

Children and young people should have the same rights to protection in the virtual world as they do in the real world. However, we know that people use the internet for grooming with the intent to exploit them sexually; we know that ICT can offer new weapons for those who bully to intimidate, threaten and harm their victims via websites, social media or text messaging; and we know that children and young people have been exposed to inappropriate content when online, which has sometimes led to their involvement in crime and anti-social behaviour.

WSCB understands the vital role that parents need to play in developing their children as responsible digital citizens and to keep them from online harm. WSCB recognises that this is not always easy and so will support parents to be the digital parents that their children need. We encourage parents to talk to their children about what they see and do online. Having an open and ongoing dialogue about their online lives, helps parents and carers talk to their children more easily about the importance of being responsible and safe. And children will feel more comfortable seeking help from them if they experience problems online.
Parents need to be ready to act if their child tells them they feel uncomfortable with something they have experienced online so we will work to ensure parents and carers are aware of different channels for reporting concerns. We will also remind parents and carers that it is equally important for them to be positive role models and that they should always display safe and responsible online behaviour themselves.

We also have a responsibility to ensure our workforce models good behaviours and are protected. The impact of Online Safety extends to all who work with young people, whether in education or social care occupations, as online applications can have a deep and long-lasting impact on professional reputations. Organisations have a duty of care towards their employees, and a staff member who is abused through the Internet may seek legal redress from their employer in some cases.

This Online Safety strategy is supported by Online Safety policy templates and documents for settings. Please consult these documents, which outline the practical aspects of the processes involved in dealing with online safety issues.
3. The issues and risks

Today’s children are citizens of a digital world. In their daily lives the use of the internet and mobile, digital technologies, represent a seamless extension of the physical world. Their emotional lives and their development are bound up in the use of these technologies. In contrast to many adults for whom these technologies are additional tools to be used for specific tasks, many of today’s children do not even notice they are using these technologies as they draw little distinction between their physical and virtual lives. As online content, social networks and instant messaging converge with mobile technology to produce lives which are always ‘on’, any line which may have existed between being online and offline is increasingly blurred.

Most parents and carers will be experiencing these changes as a revolution, albeit a disempowering one, and a barrier to communication with their children rather than an aid. This offers us a challenge. We can no longer assess the physical and emotional well-being of children and young people without considering their relationship to technology. We can no longer safeguard them without addressing the dangers which exist within the online environment.

WSCB (alongside each professional from the multi-agency network) has a statutory duty to safeguard and promote the welfare of children in Wandsworth and beyond. If we accept the challenge of the digital world then the responsibilities that come with this duty must include the development of strategies for safeguarding children within the online environment.

Safeguarding risks include:

a) Grooming
b) Cyber-bullying
c) Online pornography
d) Radicalisation (Prevent)
e) Inappropriate content
f) Youth-produced sexual imagery (sexting)
g) Self-harm
h) Online reputation
i) Privacy

a) Grooming

Grooming, or predation, can be defined as ‘befriending a child by building a strong, trusting bond’, and is most often used to refer to an act of lowering a perceived inhibitory attitude of a child regarding sexual behaviour with an adult. Typically, the grooming process involves showing pornography to the child to give the impression that sexual acts are normal, common or part of being ‘grown-up’.

The Sexual Offences Act 2003 s15(2) provides there is evidence of a clear offence when: ‘... after having met or communicated with a child on at least two earlier occasions, to meet, or travel to meet, the child with the intention of sexually abusing him or her on that occasion or later’.
A crime may be committed even without a meeting actually taking place and without the child even being involved in the meeting (eg. if a police officer has taken over the contact and pretends to be that child). Nurturing Internet friendships is not restricted to children, and there is frequent use of online chat, usually with the anticipation of real-life contact.

Online groomers are not always strangers. In many situations, a child or young person may already have met the abuser through their family or social activities. The Internet is used to build a rapport; a connection. Sometimes children are not aware they are or have been groomed, and begin to believe the abuser is their real boyfriend or girlfriend. Through the use of digital technologies, children and young people are at risk of being abused in what should be the safety of their own home by strangers.

b) Cyber-bullying

Cyber-bullying is the act of one person or a group of people using digital technology to threaten, tease, harass, upset or humiliate someone else. Bullying that happens online, using social networks, games and mobile phones, is often called cyber-bullying. It can happen anywhere; at school, at work and at home. It is usually repeated over a long period of time and can hurt a child both physically and emotionally.

In many cases, a single act can ‘go viral’ resulting in a feeling of repeated bullying as a wider audience views the abuse. The person bullying can feel a sense of anonymity and the person being bullied may not always know who is behind it. In addition, cyber-bullying provides 24-7 exposure as the nature of online activity means someone can be contacted at any time, by anyone and anywhere.

Determining a precise estimate on the number of children and young people who experience cyber-bullying has proven difficult. Prevalence rates for both victimisation and bullying perpetration range from anywhere between 5% to 80%.

A review of 35 international studies on cyber-bullying concluded that around 24% of children and young people will experience some form of cyber-bullying, and 17% will take part in cyber-bullying others.

Data collected in 2014 by Public Health England, published in 2017, shows that 17% of over 5,000 11-15 year olds had experienced cyber-bullying in the two months prior to the survey.

Children and staff can be vulnerable to online bullying via:

- Email, instant messaging (IM) and chat rooms - sending abusive or nasty messages, including sending emails to others who then participate in the bullying.
- Social networking sites, blogs - writing upsetting comments on someone’s profile and/or about people on your own status updates or tweets; uploading hurtful images or videos; setting up a fake profile dedicated to bullying someone else.
- Online gaming – inappropriate contact, abuse or harassment through multi-player gaming sites.
- Mobile phones - sending abusive texts, video or photo messages; encouraging someone to share intimate pictures or videos of themselves and then sending these on to other people (sexting). (Note: taking and keeping sexual images of anyone
under the age of 18, whether made or stored by someone over or under the age of 18 themselves, is considered a criminal offence.

Advice on what to do if bullied, includes:

- Keep copies (including screenshots) of any abusive texts, emails, social media comments or messages received with the record date and time sent. Don’t retaliate or reply.
- Block messages using the tools available and seek appropriate advice.
- If at school, be aware of and follow correct procedures. The online safety and anti-bullying policies should detail who to inform (such as the school Designated Safeguarding Lead, Headteacher, etc) and the appropriate course of action to take.

Courses of action may include any or all of the following:

- Support those affected by the bullying (by setting up a Safety Plan).
- Contact parents/carers and the local authority, as appropriate.
- Report to the police if the case is serious, e.g. involving threat or intimidation or suspected criminal activity. Report any illegal material to the Internet Watch Foundation and suspected online exploitation to CEOP (Child Exploitation Online Protection) agency.
- Be proactive. Taking a whole-school community, consistent and inclusive approach is key to effectively preventing and dealing with cases early on and ensures everyone understands the policy and procedures.
- Monitor incidents. Typically, schools log bullying incidents using their own behaviour management systems to identify trends and patterns to prevent further incidents and ensure staff are suitably trained. Schools sharing data with the local authority via the Research and Evaluation Unit (REU) help children’s services to allocate resources effectively, including training and policy development.

Although bullying in itself is not a specific criminal offence in the UK, some types of harassing or threatening behaviour. Communications such as: “sending via a public network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character”, or: “making anonymous or abusive calls” can be criminal offences under a range of different laws. These include the Protection from Harassment Act 1997, section 43 of the Telecommunications Act 1984, the Malicious Communications Act 1988, section 127 of the Communications Act 2003 and the Public Order Act 1986.

c) Online pornography

As children explore the Internet they can sometimes come across sexual content accidentally, and some of what they become exposed to may contain unpleasant and extreme images. Children may find viewing such images not only upsetting but confusing as pornography typically portrays an unrealistic image of sex and relationships. However, there are steps that should be taken to minimise the risk of exposure to this kind of inappropriate content.

Some or all of the following may suggest a child could have been viewing pornography:

- Signs of premature sexual activity, increased interest in sexuality and use of sexual language.
- Unexplained charges on their own or others (especially their parents’) bank cards.
• Switching off screens as soon as anyone comes near to the computer or phone screen.
• Inappropriate and explicit pop-ups start to appear on their computer.
• Changes in behaviour, eg. becoming much more defensive, aggressive or secretive.
• Their browser history may frequently be deleted or, if not, can reveal searches using sexual terms or sites visited that are inappropriate.

Methods to protect children from online pornography include action to:

• Block access to explicit content online, as recommended, but it shouldn’t be used as a substitute for talking about the issue.
• Set Parental Controls.
• Ensure safe search settings are activated on Google, Bing and other search engines, which all have their safety settings page. Remember to opt for the safety mode on services like YouTube and iTunes.
• Consider setting up child-friendly search engines, such as swiggle, instead of Google or Bing.
• Activate parental controls in Windows and Mac.
• Parental controls should be installed on every device a child uses: mobile phone, tablet and games consoles (both home and handheld).
• Block pop-ups if concerned about children accessing pornography accidentally this way.
• Check the search terms used in the browser history and the sites visited. If you find something that you feel is inappropriate, this can be added to your parental controls filter list. No filter is 100% effective so it is important not to rely just on this method but ensure to talk to all children about online pornography too.

**d) Radicalisation (Prevent)**

Wandsworth has been identified by the Government as a priority area for local action under the national Prevent counter-terrorism strategy. Terrorism continues to pose a threat to Wandsworth and the UK. A particular concern is the potential for UK citizens or residents to become ‘radicalised’ and drawn into becoming terrorists or supporting terrorism.

The Internet and other social media have transformed the way in which terrorist organisations communicate and recruit people to their cause. Technology allows potential perpetrators to reach a much larger audience, more quickly and provides a means of distributing and promoting violent images; instructions and messages. It can also be used to build and reinforce terrorist and extremist messages and viewpoints amongst groups through the use of online chat rooms and social media. Children and young people may be particularly susceptible to being influenced through the Internet and social media. This has potentially serious consequences for them and for the community as a whole. In addition, the publication, downloading and distribution of such material may result in prosecution under the Terrorism Act 2006.

There are a number of specific Prevent measures that should be taken locally in relation to the Internet and social media, these include:

• Increasing parent/carer awareness of the steps they can take to protect children and young people from accessing harmful content at home.
Limiting access to harmful content online in key sectors, such as schools, libraries and other public spaces.

Ensuring that action is taken to try to remove unlawful and harmful content from the internet.

Taking effective online safety action, as outlined in this document, will also assist in addressing issues of terrorism and extremism online. Additional specific information, including links to useful sources of advice and help, is available via the Wandsworth website: [Wandsworth Prevent Programme](#)

### e) Inappropriate content

What we think is inappropriate material for children may well differ from a child's view. It will also depend on a child’s age and maturity level. Inappropriate content can be defined as information or images that upset a child, material that's directed at adults, inaccurate information or information that might lead or tempt a child into unlawful or dangerous behaviour. This may include:

- 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 is no monitoring/supervision of the types of language being used, such as racist, homophobic and other forms of hate speech.

Outside of school it can be difficult to monitor what a child is viewing as they can access this material through any Internet-enabled device, including mobile ones, such as a phone or tablet. Sometimes a child may stumble upon unsuitable sites by accident, through:

- Apps they've downloaded to their mobile device.
- Links they've been sent by friends.
- Chatting to others online, or even through inter-device communication systems, such as Bluetooth.

Parents need to understand the simple, technical steps they can take to provide filtering at home and the need to be proactive in discussing these issues with their children.

### f) Youth-produced sexual imagery (sexing)

According to the latest guidance from the United Kingdom Council for Child Internet Safety (UKCCIS 2016), sexting is defined as ‘the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18’. It includes nude or nearly nude images and/or sexual acts. It is also referred to as ‘youth-produced sexual imagery’.

'Sexting' does not include the sharing of sexual photos and videos of under-18s with or by adults. This is a form of child sexual abuse and must be referred to the police.
A 2016 NSPCC/Office of the Children’s Commissioner England study found that just over one in ten boys and girls (13%) had taken topless pictures of themselves. Around one in four of those were girls and 3% had taken fully naked pictures. Of those who had taken sexual images, 55% had shared them with others. 31% of this group had also shared the image with someone that they did not know.

What to do if an incident involving ‘sexting’ comes to your attention:

- Report it to your Designated Safeguarding Lead (DSL) immediately.
- Never view, download or share the imagery yourself, or ask a child to share or download. This is illegal.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- Do not share information about the incident to other members of staff or the young person(s) it involves. Contact with parents needs to be agreed with the DSL and, possibly, the police or social care professionals.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

**g) Self-harm**

There are many reasons why young people may start to self-harm. Family reasons, such as not getting on with other family members or their parents getting divorced, may be a trigger. They may have personal problems to do with sexuality, race, culture or religion, or they may suffer from low self-esteem and feelings of isolation. Bereavement, current or previous experience of abuse in childhood or stress as a result of bullying or impending exams can all lead to self-harm.

There are two types of self-harm: physical and emotional, and young people will go to great lengths to hide them or explain them away.

The signs to look for with physical self-harm are cuts, bruises, burns and bald patches from hair pulling. Young people are likely to cover themselves up in long-sleeved clothes and hats to hide the signs.

The emotional signs include: depression, tearfulness and low motivation, unusual eating habits, sudden weight loss or gain, low self-esteem and drinking or taking drugs. Experts say self-harm behaviour normally ends within five years of starting, however, for some, it can last into adulthood.

The increase in awareness of self-harm generally has seen a corresponding rise in the number of websites covering the issue – both positive and negative. Cyberbullying and other forms of online abuse can drive young people to self-harm, whilst pro-self-harm websites or communities that spread knowledge of self-harming techniques can encourage experimentation. There are however a number of excellent sites that discourage this and offer advice, guidance and knowledge to help children deal with this issue.

**h) 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 digital footprint or
online reputation. It is important young people understand how to manage their online reputation and the potential impact a negative online reputation may have on their future, including employment prospects.

Young people start sharing information from a young age. The result is that by the time they are 18 years of age, a permanent and often substantial record will exist about them. What happens if that information is inaccurate, or is the result of sexting or bullying? Once uploaded, such information is difficult to erase or change and could have a long-lasting impact.

1) Privacy and identity theft
In the online world, young people could unwittingly reveal enough personal details like their address and telephone number to enable their identity to be stolen. It is therefore paramount that they know how to keep their private information private.

If a young person’s identity is stolen it may not be noticed for many years and could in some cases lead to them being the victim of blackmail, grooming or bullying.
We may start to suspect a young person’s identity has been stolen if they:

- Receive a bill for something they haven’t ordered.
- Start to get emails from an organisation they don’t recognise.
- Receive any letters regarding government benefits or tax payments.

Examples of how to help keep children safe online include:

- Checking the privacy settings for every social networking site and app a young person has signed up to. Agree with them what they’ll share, and with whom.
- Check the privacy settings on their smartphone and tablet devices. Things to look out for are whether they are set up for location services, sharing of contacts, photos and calendars, bluetooth sharing, microphone, video and advertising.
- Search the child’s full name in several search engines and see what information and photographs are public.
- If you find any inaccurate comments or photographs that might damage a child’s reputation, ask the website on which they appear to remove them.

If a child’s identity has been stolen:

- Tell any affected websites about the problem.
- The child should log in and change their password immediately.
- If they can’t log in, contact the website’s technical support department for help.
- Change any security questions or additional information sites ask for to verify the child’s identity.

If a child has become the victim of fraud report it to Action Fraud

The new Data Protection Act 2018 and the EU General Data Protection Regulation came into effect in 2018. Together they provide greater rights and protection for children and aim to prevent companies marketing to, profiting from and profiling or otherwise exploiting a child’s data under the age of 13. Alongside the law change we need to substantially improve digital literacy education for all children so that they understand the importance of their online privacy and how to maintain and enforce it.
4. How we will tackle Online Safety issues

Policies and Practices
We will develop effective policies and practices at both at WSCB and service-level to protect and inform our children and their parents to maximise the opportunities from technology and to minimise the potential negative impact of technologies.

Online Safety should be taken in to account in the following policies, resources and guidance:

- Safeguarding and child protection policy.
- Teaching and learning (curriculum) policy.
- Anti-bullying policy.
- Behaviour policy.
- Acceptable use policy
- Prevent strategy.
- Data protection policy.

Infrastructure and technology
Infrastructure and technology has a key role to play in helping to protect our young people. Tools are available which can automate the process of monitoring and recording most internet activity. The management of these tools must be purposeful and effective and support policy and practice. We will support schools to provide safe infrastructure and environments for learning and help parents who require assistance in making their home environment safe for online activity.

Education and training
All staff dealing directly with children and young people have a role to play in making sure young people are educated to become responsible digital citizens.

Professionals need to be aware of the risks facing young people and will be provided with a range of strategies to enable them to teach and promote responsible use of technologies. Professionals also need to be aware of the great wealth of opportunities there are for young people using technologies to fully understand why this is so important.

Information, advice and support are similarly available for parents and carers, whether in schools or settings such as Children’s Centres, etc.

Review and develop
Services will be encouraged to review and evaluate their provision for Online Safety education. In addition, all organisations should also regularly review their policy and strategies, as well as ensure their staff are up to date with the latest developments and resources.
5. Local governance – Online Safety in Wandsworth

The WSCB is made up of representatives from a range of partner agencies. WSCB will form an Online Safety working group that will be tasked to review and revise the Online Safety Strategy and Policy periodically. The group will consist of representatives from relevant partner agencies.

The WSCB Business Manager takes the lead role of coordinating the Online Safety working group and facilitates meetings. The Online Safety working group will present revised and updated documents to the Monitoring Sub-Committee and WSCB for ratification as timetabled. The WSCB Executive will sign off all strategies and policies, committing their agencies to working in partnership accordingly.

The WSCB online safety working group will:

- Be a central point of contact for guidance, advice and networking in relation to Online Safety issues.
- Ensure the views of children and young people are at the heart of everything it does through participation work involving school councils and the Youth Council, etc.
- Revise and set out the roles and responsibilities of the Online Safety safeguarding lead officers (An online safety safeguarding lead officer could be the person within the organisation or agency that has lead responsibility for safeguarding or a separate person who has an understanding of safeguarding issues who can fulfil this role).
- Update and manage a network of these officers who can work within their agencies to raise awareness and understanding. Contact details of lead officers will be available online via www.wscb.org.uk.
- Liaise with the Safeguarding Training sub-group to ensure the delivery and quality assurance of multi-agency Online Safety training.
- Identify and signpost the Online Safety Policy, the resources available and, where necessary, develop them, for example:
  - Recommend appropriate web filtering/monitoring tools.
  - Design educational resources for teachers, and
  - Inform parents and carers about the latest developments.
- Report back to WSCB via the Monitoring Sub-Committee.
- Enable agencies, through the incorporation of the Online Safety strategy into their existing safeguarding policies, to ensure that they have robust procedures in place in relation to recognition, identification, reporting and appropriate response to online safety issues.
6. Roles and responsibilities

Online Safety is recognised as an important aspect of strategic leadership in Wandsworth. The independent chair of WSCB, with the support of all partner organisations and staff, aims to embed safe practices into our work. WSCB ensures that this strategy is implemented and compliance with it monitored.

Wandsworth’s ‘Online Safety Co-ordinator’ role will be fulfilled by the ‘Online Safety Working Group’. Membership is outlined within the Online Safety Strategy or can be accessed via the website at www.wscb.org.uk.

Our Online Safety Co-ordinator ensures they keep up to date with Online Safety issues and guidance through liaison with organisations such as LGfL (London Grid for Learning) and the CEOP (Child Exploitation and Online Protection) agency. The Online Safety C-ordinator ensures the WSCB, Director of Children’s Services, senior management and Council members are updated as necessary.

All staff that work with children are responsible for promoting and supporting safe behaviours and following Online Safety procedures. Central to this is fostering a ‘No Blame’ culture so children and young people feel able to report any bullying, abuse or inappropriate materials, with a restorative approach followed to ensure the voice of the person harmed is heard and changes to abusive behaviours facilitated.

All staff should be familiar with this strategy including:

- Safe use of e-mail.
- Safe internet use, including the use of internet-based communication services, such as instant messaging and social media.
- Safe use of network, equipment and data.
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras.
- Publication of child information/photographs and use of websites.
- Cyber-bullying prevention and intervention procedures.
- Their role in providing Online Safety education for children and young people.
7. WSBC Strategic Priorities

WSCB has set 4 key safeguarding priorities for 2016-18:

- **Early Help**: Ensure services provide appropriate early help and intervention, consistent application of thresholds between preventative, targeted and specialist services and monitor the effectiveness of the Multi-agency Safeguarding Hub (MASH).

- **Children and Young People**: Address the challenges and risks faced by vulnerable children and young people, in particular:
  - Going missing from care, education and home
  - Child Sexual Exploitation
  - Radicalisation
  - Self-harming behaviour
  - Involvement in gangs
  - Children with disabilities and special educational needs
  - Female genital mutilation
  - Honour Based Violence
  - Forced Marriage

- **Neglect**: Ensure that the issue of neglect receives due prominence in assessment, prevention and intervention work especially where there are concerns of:
  - Domestic abuse
  - Parental mental health
  - Substance misuse

- **Children living away from their parents**: Ensure children not living at home are safe, receive high quality support to achieve better outcomes, which includes:
  - Children Looked After
  - Privately fostered children
  - ‘Sofa surfing’
  - Unaccompanied minors/young people in custody

8. Monitoring and evaluation

Online Safety is relevant to all priority areas of the WSCB in one way or another. For monitoring and reporting purposes this strategy will be linked to Priority 2. All agencies will be responsible for overseeing the implementation of actions to address this area of focus and report to the WSCB through the monitoring sub-committee. The Online Safety working group will report annually to the WSCB on progress against objectives, prioritising outcomes on ‘what difference we have made to the lives of children and young people’.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APRF</td>
<td>Annual Planning and Review Forum</td>
</tr>
<tr>
<td>CEOP</td>
<td>Child Exploitation and On-Line Protection</td>
</tr>
<tr>
<td>DESS</td>
<td>Department for Education and Social Services</td>
</tr>
<tr>
<td>FGM</td>
<td>Female Genital Mutilation</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>LADO</td>
<td>Local Authority Designated Officer</td>
</tr>
<tr>
<td>LGfL</td>
<td>London Grid for Learning</td>
</tr>
<tr>
<td>LSCB</td>
<td>Local Safeguarding Children Board</td>
</tr>
<tr>
<td>MASH</td>
<td>Multi Agency Safeguarding Hub</td>
</tr>
<tr>
<td>RBC</td>
<td>Regional Broadband Consortia (LGfL in London)</td>
</tr>
<tr>
<td>VAWGS</td>
<td>Violence Against Women and Girls Strategy</td>
</tr>
<tr>
<td>WSCB</td>
<td>Wandsworth Safeguarding Children Board</td>
</tr>
</tbody>
</table>
10. Appendix 2 - What do we do if?

An inappropriate website is accessed *unintentionally* in a school or children’s setting by staff or a child:

1. Play the situation down; don’t make it into a drama.
2. Report to the head/senior manager/online safety lead officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school or organisation’s technical support and ensure the site is filtered.
4. If a Wandsworth Schools ICT supported school, contact editsupport@wandsworth.gov.uk or phone 020 88718373.
5. Inform Wandsworth’s Online Safety officer if the filtering service is provided via the LA/RBC.

An inappropriate website is accessed *intentionally* by a child:

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents/carer of the child.
3. Inform the organisation’s technical support and ensure the site is filtered if need be. If a Wandsworth Schools ICT supported school, contact editsupport@wandsworth.gov.uk or phone 020 88718373.
4. Inform Wandsworth’s Online Safety officer if the filtering service is provided via the LA/RBC.

An adult uses an organisation's ICT equipment inappropriately:

1. Ensure you have a colleague with you. Do not view the misuse alone.
2. Report the misuse immediately to the head/senior manager/Online Safety officer and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head/senior manager/Online Safety officer should then:
4. Remove the PC to a secure place.
5. Instigate an audit of all ICT equipment by the ICT technical support providers to ensure there is no risk of others accessing inappropriate materials.
6. Identify the precise details of the material.
7. Contact the LADO for advice – a referral may be needed
8. Take appropriate disciplinary action. (contact Personnel/Human Resources)
9. In an extreme case where the material is of an illegal nature:
10. Remove the PC to a secure place and document what you have done.
11. Contact the local police and follow their advice.

A bullying incident directed at a child occurs through email or mobile phone technology:

1. Advise the child not to respond to the message.
2. Refer to relevant policies including Online Safety and anti-bullying, and apply appropriate sanctions and/or support.
4. Inform the sender’s e-mail service provider.
5. Notify parents/carers of the children involved.
6. Consider organising a parent/carer workshop for the community.
7. Inform the police if necessary.
8. Record all incidences and submit annual data returns to the Research and Evaluation Unit (REU), as requested.

Malicious or threatening comments are posted on an Internet site about a child or member of staff:

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform Wandsworth’s Online Safety officer.

You are concerned that a child’s safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

1. Report to and discuss with the named child protection officer/lead officer for safeguarding and contact parents/carers.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement of police and Social Services.
5. Inform Wandsworth’s Online Safety officer.
6. If adult has contact with child or other children in a professional context refer to the LADO.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.
11. Appendix 3 - Legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of a child to 18 years old;
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Criminal Justice and Courts Act (amendment Oct 2014) created a specific offence of distributing a private sexual image of someone without their consent and with the intention of causing them distress (commonly called "revenge porn"). The maximum custodial sentence is two years.

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.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (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.

N.B. Schools should already have a copy of “Children & Families: Safe from Sexual Crime” document as part of their child protection packs.

Communications Act 2003 (section 127)
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.

Data Protection Act 2018 and the General Data Protection Regulation

The Act and Regulation requires anyone who handles personal information to notify the Information Commissioner’s Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual’s motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else’s password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission.

The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

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.

Protection of Children Act 1978 (Section 1)
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.

**Obscene Publications Act 1959 and 1964**
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

**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.

The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

**Keeping Children Safe in Education 2018**
Sets out what schools and colleges in England must do to safeguard and promote the welfare of children and young people under the age of 18. Annex C provides Online Safety information and support.
12. Appendix 4 – LGfL School Online Safety Policy template

NOTE: This policy has elements marked in yellow needing customisation or which may not apply in your school. The policy also has statements which contradict each other because the statements cover a range of situations regarding your school’s approach to pupil or staff use of mobile and hand held devices.

This policy is not permitted for use without adapting/editing to suit your school/setting.

<table>
<thead>
<tr>
<th>School logo</th>
<th>Name of School</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy review Date</td>
<td></td>
</tr>
<tr>
<td>Date of next Review</td>
<td></td>
</tr>
<tr>
<td>Who reviewed this policy?</td>
<td></td>
</tr>
</tbody>
</table>

This policy is part of the School’s Statutory Safeguarding Policy. Any issues and concerns with Online Safety must follow the school’s safeguarding and child protection processes.

LGfL School Online Safety Policy Template

Contents

1. Introduction and Overview
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy is communicated to staff/pupils/community
   - Handling complaints
   - Reviewing and Monitoring

2. Education and Curriculum
   - Pupil online safety curriculum
   - Staff and governor training
   - Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure
- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data Security
- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content
- Personal mobile phones and devices
- Digital images and video

Appendices (download these documents as a zip file from osappendices.lgfl.net):
A1: Acceptable Use Agreement (Staff, Volunteers and Governors)
A2: Acceptable Use Agreements (Pupils – adapted for phase)
A3: Acceptable Use Agreement including photo/video permission (Parents)
A4: Protocol for responding to online safety incidents
   http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements
A5: Prevent: Radicalisation and Extremism
A6: Data security: Use of IT systems and Data transfer
   Search and Confiscation guidance from DfE
1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Name of school with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable, that this is viewed as a safeguarding issue and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)
Scope

This policy applies to all members of [Name of school] community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of [school/academy] IT systems, both in and out of [Name of school].

Roles and responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
</table>
| Headteacher                                                         | • Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance  
• To lead a ‘safeguarding’ culture, ensuring that online safety is fully integrated with whole school safeguarding.  
• To take overall responsibility for online safety provision.  
• To take overall responsibility for data management and information security (SIRO) ensuring school’s provision follows best practice in information handling.  
• To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services  
• To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.  
• To be aware of procedures to be followed in the event of a serious online safety incident.  
• Ensure suitable ‘risk assessments’ undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.  
• To receive regular monitoring reports from the Online Safety Co-ordinator.  
• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager.  
• To ensure Governors are regularly updated on the nature and effectiveness of the school’s arrangements for online safety.  
• To ensure school website includes relevant information. |
| Online Safety Co-ordinator/Designated Child Protection Lead (This may be the same person) | • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school’s online safety policy/documents.  
• Promote an awareness and commitment to online safety throughout the school community.  
• Ensure that online safety education is embedded within the curriculum. |
<table>
<thead>
<tr>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
</table>
| **Governors/Safeguarding governor (including online safety)**       | • To ensure that the school has in place policies and practices to keep the children and staff safe online  
• To approve the Online Safety Policy and review the effectiveness of the policy  
• To support the school in encouraging parents and the wider community to become engaged in online safety activities  
• The role of the online safety Governor will include: regular review with the online safety Co-ordinator.                                                                                                                                                                                                                                                                                                                                 |
| **Computing Curriculum Leader**                                      | • To oversee the delivery of the online safety element of the Computing curriculum                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| **Network Manager/technician**                                       | • To report online safety related issues that come to their attention, to the Online Safety Coordinator  
• To manage the school’s computer systems, ensuring - school password policy is strictly adhered to.  
- systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)  
- access controls/encryption exist to protect personal and sensitive information held on school-owned devices  
- the school’s policy on web filtering is applied and updated on a regular basis  
• That they keep up to date with the school’s online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant  
• That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher  
• To ensure appropriate backup procedures and disaster recovery procedures are in place and regularly updated.                                                                                                                                                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>recovery plans are in place</td>
</tr>
<tr>
<td></td>
<td>• To keep up-to-date documentation of the school’s online security and technical procedures</td>
</tr>
<tr>
<td>Data and Information (Asset Owners) Managers (IAOs)</td>
<td>• To ensure that the data they manage is accurate and up-to-date</td>
</tr>
<tr>
<td></td>
<td>• Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.</td>
</tr>
<tr>
<td></td>
<td>• The school must be registered with Information Commissioner</td>
</tr>
<tr>
<td>LGfL Nominated contact(s)</td>
<td>• To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant</td>
</tr>
<tr>
<td>Teachers</td>
<td>• To embed online safety in the curriculum</td>
</tr>
<tr>
<td></td>
<td>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)</td>
</tr>
<tr>
<td></td>
<td>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws</td>
</tr>
<tr>
<td>All staff, volunteers and contractors.</td>
<td>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction.</td>
</tr>
<tr>
<td></td>
<td>• To report any suspected misuse or problem to the online safety coordinator</td>
</tr>
<tr>
<td></td>
<td>• To maintain an awareness of current online safety issues and guidance e.g. through CPD</td>
</tr>
<tr>
<td></td>
<td>• To model safe, responsible and professional behaviours in their own use of technology</td>
</tr>
<tr>
<td><strong>Exit strategy</strong></td>
<td>• At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.</td>
</tr>
<tr>
<td>Pupils</td>
<td>• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually</td>
</tr>
<tr>
<td></td>
<td>• To understand the importance of reporting abuse, misuse or access to inappropriate materials</td>
</tr>
<tr>
<td></td>
<td>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology</td>
</tr>
<tr>
<td></td>
<td>• To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out</td>
</tr>
<tr>
<td>Role</td>
<td>Key Responsibilities</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>of school and realise that the school’s online safety policy covers their actions out of school</td>
<td>• To contribute to any ‘pupil voice’ / surveys that gathers information of their online experiences</td>
</tr>
</tbody>
</table>
| Parents/carers                                 | • **To read, understand and promote the school’s Pupil Acceptable Use Agreement with their child/ren**  
• to consult with the school if they have any concerns about their children’s use of technology  
• to support the school in promoting online safety and endorse the Parents’ Acceptable Use Agreement which includes the pupils’ use of the Internet and the school’s use of photographic and video images |
| External groups including Parent groups         | • Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school  
• to support the school in promoting online safety  
• To model safe, responsible and positive behaviours in their own use of technology. |
Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school [website/staffroom/classrooms].
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer).

Handling a sexting/nude selfie incident:

[UKCCIS “Sexting in schools and colleges”](#) should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people

  *When assessing the risks the following should be considered:*
  
  o Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  o Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  o Are there any adults involved in the sharing of imagery?
  o What is the impact on the pupils involved?
  o Do the pupils involved have additional vulnerabilities?
  o Does the young person understand consent?
  o Has the young person taken part in this kind of activity before?

- If a referral should be made to the police and/or children’s social care
• If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
• What further information is required to decide on the best response
• Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
• Whether immediate action should be taken to delete or remove images from devices or online services
• Any relevant facts about the young people involved which would influence risk assessment
• If there is a need to contact another school, college, setting or individual
• Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children’s social care should be made if at this initial stage:
1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person’s developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police but in most cases a referral should be made to the MASH as there may be other information that the school are unaware of.

The decision to respond to the incident without involving the police or children’s social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school’s pastoral support and disciplinary framework and if appropriate local network of support.

**Reviewing and Monitoring Online Safety**

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

• The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
• There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils
2. Education and Curriculum

Pupil Online Safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the *Computing curriculum/PSHE and other curriculum areas as relevant*. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school’s online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school’s Acceptable Use Agreements.

Parent awareness and training

This school:

- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.
3. Expected Conduct and Incident management

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors:

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/carers:

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school’s ‘rules of appropriate use for the whole school community’ are and what sanctions result from misuse.
Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school’s escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved ‘web filtering management’ status;
- uses USO user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send ‘protect-level’ (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access ‘protect-level’ (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school:
• uses individual, audited log-ins for all users - the LGfL USO system.
• uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
• uses teacher ‘remote’ management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful.
• has additional local network monitoring/auditing software installed.
• ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies.
• has daily back-up of school data (admin and curriculum).
• uses secure, ‘Cloud’ storage for data back-up that conforms to DfE guidance.
• storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:
• ensures staff read and sign that they have understood the school’s online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school’s network / We also provide a different/use the same username and password for access to our school’s network.
• all pupils have their own unique username and password which gives them access to the Internet and other services.
• makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins.
• has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
• requires all users to log off when they have finished working or are leaving the computer unattended.
• ensures all equipment owned by the school and/or connected to the network has up to date virus protection.
• makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
• makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
• maintains equipment to ensure Health and Safety is followed.
• ensures that access to the school’s network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems.
• does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems.
• has a clear disaster recovery system in place that includes a secure, remote off site back up of data.

• this school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools.

• ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX).

• our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.

• all IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

**Password policy**

This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.

All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

We require staff to use **STRONG passwords.**

We require staff to change their passwords into the MIS, LGfL USO admin site, **every 90 days/twice a year.**

We require staff using critical systems to use two factor authentication.

**E-mail**

This school:

• provides staff with an email account for their professional use, London Staffmail/LA email and makes clear personal email should be through a separate account.

• we use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk/head@schoolname.la.sch.uk/or class e-mail addresses.

• will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

• will ensure that email accounts are maintained and up to date.

• we use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

• will use the LGfL pupil email system which is intentionally ‘anonymised’ for pupil protection.

• are taught about the Online Safety ‘netiquette’ of using e-mail both in school and at home.
Staff:
- can only use the LA or LGfL e-mail systems on the school system.
- will use LA or LGfL e-mail systems for professional purposes.
- access in school to external personal e-mail accounts may be blocked.
- never use email to transfer staff or pupil personal data. ‘Protect-level’ data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website
- The headteacher, supported by the governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school website complies with statutory DFE requirements.
- Most material is the school’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author’s identity or status.
- Photographs published on the web do not have full names attached. We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website.

Cloud Environments
- Uploading of information on the schools’ online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the school’s online environment will only be accessible by members of the school community.
- In school, pupils are only able to upload and publish within school approved ‘Cloud’ systems.
Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- For the use of any school approved social networking will adhere to school’s communications policy.

School staff will ensure that in private use

- No reference should be made in social media to students/pupils, parents/carers or school staff.
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school/academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents/carers:

- are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.
• We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

• the headteacher is the Senior Information Risk Officer (SIRO).
• staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
• we ensure staff know who to report any incidents where data protection may have been compromised.
• all staff are DBS checked and records are held in a single central record

Technical solutions

• Staff have secure area(s) on the network to store sensitive files.
• We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
• We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
• All servers are in lockable locations and managed by DBS-checked staff.
• Details of all school-owned hardware will be recorded in a hardware inventory.
• Details of all school-owned software will be recorded in a software inventory.
• Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
• Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
• We are using secure file deletion software.
6. Equipment and Digital Content

The policy also has statements which contradict each other because the statements cover a range of situations. **This policy cannot be used without editing to suit your school/setting.**

**Mobile Devices (mobile phones, tablets and other mobile devices)**

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets. ‘Mobile-free’ signs to this effect are displayed.

- All mobile devices will be handed in at reception should they be brought into school.

- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.

- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.

- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.

- Personal mobile devices will only be used during lessons with permission from the teacher.

- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

- Staff members may use their phones during school break times.

- All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles
devices may be searched at any time as part of routine monitoring. <Search processes are detailed in the Behaviour Policy>.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

**Storage, Synching and Access**

**The device is accessed with a school owned account**

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.

- PIN access to the device must always be known by the network manager.

**The device is accessed with a personal account**

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.

- PIN access to the device must always be known by the network manager.

- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

**Students’ use of personal devices**

- The school strongly advises that student mobile phones and devices should not be brought into school.

- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.

- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student’s withdrawal from either that examination or all examinations.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to ‘silent’ mode. Bluetooth communication should be ‘hidden’ or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- we gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually).
- we do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- if specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.
• the school blocks/filter access to social networking sites unless there is a specific approved educational purpose.

• pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work.

• pupils are advised to be very careful about placing any personal photos on any ‘social’ online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

• pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.
13. Appendix 5 – Cyber-bullying

What is cyber-bullying?

“Cyber-bullying is bullying using technology eg. prank calls, sending nasty text messages and posting on hate sites, as well as forwarding hurtful emails or sending around humiliating videos”

Beatbullying

Technology can be used as a way to bully someone because of their race, religion, gender, sexuality, disability, etc.

Cyber-bullying can involve wider Online Safety risks, including:

- Threats and intimidation by mobile phone, email, or online.
- Harassment or stalking - repeated, prolonged, unwanted contact or monitoring of another person.
- Prejudice-based bullying - these may be general insults or racist, homophobic, biphobic, transphobic (HBT), disabilist or sexist remarks.
- Excluding others - setting up a closed group, refusing to acknowledge one user on purpose.
- Identity theft, unauthorised access and impersonation - ‘hacking’ by finding out or guessing a username and password.
- Publicly posting, sending or forwarding information or images - disclosing information on a website.
- Manipulation – this may involve getting people to behave in an inappropriate, provocative/sexual way.
- Sexting - sending sexually explicit photographs or messages via mobile phone.
- Trolling - a provocative email or posting intending to incite an angry response.
- Cyber-baiting - inciting a teacher to lose his or her temper while filming it on a mobile phone. The video might be then uploaded onto the internet to embarrass the teacher and the school.
- Fraping – a compound of Facebook and rape, describing someone’s social networking profile being hacked into and changed.
- Ratting - a remote access Trojan (RAT) is a malware program that allows administrative control over the target computer.
- Click-jacking – this is a malicious technique used to trick the user into clicking on something different from what the user thinks they are clicking onto. This might make the user vulnerable to giving confidential information or remotely taking control of their computer.

Children, young people and adults can be cyber-bullied via:

- Text messages.
- Picture/video clips (via mobile phone cameras).
- Phone calls (via mobile phone).
- Emails.
- Chat-rooms.
- Instant messaging.
- Websites and social media (eg Twitter, Facebook, Instagram, etc).
Cyber-bullying and the law
There is not a specific law which makes cyber-bullying illegal but it can be considered a criminal offence under several acts, including:


What you can do
If you, or someone you know, is being cyber-bullied, tell a trusted adult in the first instance. This could be:

- At home – a parent or carer, brother or sister, another member of your family (eg. aunt, uncle or grandparent).
- At school – a friend, playground buddy or peer mentor, teacher, form tutor, head of year, a member of support staff (eg. teaching assistant / learning support assistant, Learning Mentor).
- Member of the community – a police officer, PCSO, road crossing guide, community/faith leader.
- On-line – children and young people can contact someone in confidence at ChildLine [www.childline.org.uk](http://www.childline.org.uk).

If you’re being bullied online/by text:
- Preserve the evidence - save the messages/material.
- Tell a parent or other trusted adult or report it online as above.
- Do not retaliate or reply.
- If possible, block the person.

If you see bullying online/by text:
- Report it to a parent, trusted adult or teacher
- Support the victim - imagine how you would feel if you were being bullied

Advice for parents and carers:
- Your child is just as likely to bully as being a target of bullying
- Watch out for uncharacteristic behaviours (eg. your child being upset or secretive, becoming isolated and withdrawn, using the phone/internet more than usual, changing friendship groups).
- Remind your child not to retaliate and keep any evidence (eg. text messages, screen shots, photos, etc).

- Report the bullying – contact the school if the bullying involves another pupil and contact your service provider to report the user and remove the content. If the bullying is more serious and a potential criminal offence, consider contacting CEOP [www.ceop.police.uk](http://www.ceop.police.uk) or the police
Advice for professionals working with children and young people:
- If you yourself are a target of on-line abuse and you work with children and young people, call the UK Safer Internet Centre helpline on 0344 381 4772 (calls on this number are charged at local call rate) Monday to Friday 10.00am – 4.00pm. You can also email helpline@saferinternet.org.uk for help anytime. More information is available on the website: www.saferinternet.org.uk

Useful documents for staff and professionals

Department for Education
Preventing and tackling bullying

Ofsted
Inspecting Online Safety

Workplace bullying
ACAS (Advisory, Conciliation and Arbitration Service) www.acas.org.uk

ATL (Association of Teachers & Lecturers) www.atl.org.uk

Dignity at Work www.dignityatwork.org

GMB www.gmb.org.uk

Gov.UK www.gov.uk

NASUWT www.nasuwt.org.uk

National Union of Teachers www.teachers.org.uk

TUC (Trade Union Congress) www.tuc.org.uk

Unison www.unison.org.uk
Useful websites for children, young people and parents/carers

**Cyber-bullying**
CEOP (Child Exploitation On-line Protection) [www.ceop.police.uk](http://www.ceop.police.uk)  [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
Childnet [www.childnet-int.org](http://www.childnet-int.org)
Cybermentors (Beat Bullying) [www.beatbullying.org/dox/what-we-do/cybermentors.html](http://www.beatbullying.org/dox/what-we-do/cybermentors.html)
Digizen [www.digizen.org](http://www.digizen.org)
Kidsmart [www.kidsmart.org.uk](http://www.kidsmart.org.uk)
BBC [www.bbc.co.uk/webwise](http://www.bbc.co.uk/webwise)
Internet Watch Foundation [www.iwf.org.uk](http://www.iwf.org.uk)
GetNetWise [www.getnetwise.org](http://www.getnetwise.org)
Fearless (Junior Crimestoppers) [www.fearless.org](http://www.fearless.org)

**Disabilist bullying**
Mencap [www.mencap.org.uk](http://www.mencap.org.uk)
Contact a Family [www.cafamily.org](http://www.cafamily.org)

**Homophobic bullying**
Albert Kennedy Trust [www.akt.org.uk](http://www.akt.org.uk)
EACH (Educational Action Challenging Homophobia) [www.eachaction.org.uk](http://www.eachaction.org.uk)
Rainbow Project [www.rainbow-project.org](http://www.rainbow-project.org)
Schools Out [www.schools-out.org.uk](http://www.schools-out.org.uk)
Stonewall [www.stonewall.org.uk](http://www.stonewall.org.uk)

**Racist bullying**
Show Racism the Red Card [www.srtrc.org](http://www.srtrc.org)

**Sexist, sexual and transphobic bullying**
End Violence Against Women [www.endviolenceagainstwomen.org.uk](http://www.endviolenceagainstwomen.org.uk)
Mermaids [www.mermaidsuk.org.uk](http://www.mermaidsuk.org.uk)
GIRES (Gender Identity Research & Education Society) [www.gires.org.uk](http://www.gires.org.uk)
14. Appendix 6 – Online Safety contacts, links and further information

Online Safety working group:

Gary Hipple
Head of Schools ICT, Children’s Services
Email: ghipple@wandsworth.gov.uk

Mark Holliday
Deputy Head of Education Inclusion Service, Children's Services
Email: mholliday@wandsworth.gov.uk

Kaied Ghiyatha
Interim WSCB Manager
Tel. 020 8871 8610
Email: wscb@wscb.org.uk or wscb@wandsworth.gov.uk

Alex Purssey
City Learning Centre
Email: alex.purssey@wandsworthclc.org

Stella Macauley
Safeguarding in Education Officer
Email: smacauley@wandsworth.gov.uk

Wandsworth Children’s Services - Online Safety Officer
e-mail: esafety@wandsworth.gov.uk
Tel: 0208 8718373

Wandsworth Children's Services ICT Support
*Help with filtering and network security.*
Tel: 0208 8718373

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk

Online Safety in Schools
http://www.clusterweb.org.uk?esafety
Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

Kidsmart
http://www.kidsmart.org.uk/

London Grid for Learning Online Safety resources
http://safety.lgfl.net including One Minute guide

NCH – The Children’s Charity

NSPCC

Safer Internet Centre
http://www.saferinternet.org.uk

Stop Text Bully
www.stoptextbully.com

Think U Know website
http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

Support for children visiting pro-anorexia websites
http://www.b-eat.co.uk/

Support for children visiting suicide websites
(this is initial work on this important area, but Samaritans can provide specific support)