London Borough of Merton

Report and Recommendations arising from the Scrutiny Review of Online Strategies in Schools

Children and Young People Overview & Scrutiny Panel

September 2015

Task Group Members

Cllr Katy Neep (Chair)
Cllr James Holmes (Vice Chair)
Cllr Joan Henry

Co-opted members

Peter Connellan
Denis Popovs

Scrutiny Support
Rebecca Redman, Scrutiny Officer

For further information relating to the review, please contact:
Scrutiny Team
London Borough of Merton
Merton Civic Centre
London Road
Morden
Surrey SM4 5DX
Tel: 020 8545 3864
E-mail: scrutiny@merton.gov.uk

Acknowledgements

We would like to thank all the officers and external witnesses who have taken the time to provide written and verbal information and discussed their ideas with us. All contributors are listed in Appendix 1 of this report.

Foreword by Councillor Katy Neep - Chair of the Online Strategies in Schools Task Group

It is important in this changing world of online technologies and innovations that we ensure our young people access the latest developments and use them to enhance their learning and development.

However it is clear from both the media and this short task group review that there are some lessons to be learnt around the support, advice and guidance that we provide our young people whilst they are online. This was particularly evident when looking at the potential impact that online presence can have on job roles and interviews in later life.

All contributions to the task group have been informative, engaging and insightful. Each one providing us with either a new idea or verification that the recommendations that we had started to form fulfilled their specific needs.

A special thanks should go to the young people who have helped shape this report and provided us with an insight into how they use the online world and the impact it has on them. We all really enjoyed these workshops and hope we have captured their vision in this report.

Our thanks also go to officers at the council who have done a sterling job in pulling together workshops, interviews and the vast reports that have guided and informed us throughout. Specific thanks go to Rebecca Redman without whom this report literally would not be written.

My thanks as Chair of my first task group goes to my fellow contributors and Vice Chair who have supported and encouraged me as I hone my Chairing skills. I look forward to working with officers and the Cabinet member to implement the recommendations and ensure that our young people build successful, safe and inspirational lives both off and online.

Executive Summary

The Children and Young People Scrutiny Panel set up a task group to review the mechanisms in place within schools in the borough to support young people and mitigate any potential risks to their safety when online. This issue was felt to be important because it touched upon a number of issues and challenges which have been made prominent by Government, the media, schools, parents and other organisations.

The task group agreed that this review should be a short piece of work that would focus specifically on the role that schools play in managing young people's exposure to risk when online, and to establish how they might be better supported by the council. The task group engaged a range of stakeholders in this review in order to hear first hand what experiences head teachers, governors, young people and the police had of e-safety and both the positive and negative uses of the internet for children and young people. The task group also sought to establish how e-safety considerations and measures have been embedded into school policy, practice and culture.

Expertise in this area was also sought through accessing research undertaken and guidance and good practice provided by the following organisations/government publications:

- UK Council for Child Internet Safety (UKCCIS)
- London School of Economics (LSE)
- EU Kids Online Network
- London Grid for Learning (LGfL)
- Byron Review – Safer Children in a Digital World (2008)

The focus of the task group's recommendations are on:

- All schools having a robust e-safety strategy that is regularly monitored and refreshed;
- Parents being equipped with the necessary skills to support their children in their online experiences;
- Building young peoples resilience and ability to respond appropriately to e-safety risks;
- Young people being empowered to act responsibly and safely when online to ensure positive use of the internet can be utilised to aid learning, the development of peer

relationships, and promote creativity, so that young people develop skills which lead to employment opportunities;

- An increased role for governors in supporting schools and undertaking a more frequent performance monitoring role in determining the effectiveness of e-safety policies within schools;
- Awareness raising and education for young people and parents, in particular, education earlier on e-safety issues with much younger children; and
- The use of technology, such as apps, that can be employed as an information tool for parents

The task group wishes to take forward these recommendations in consultation with schools, governors and the Merton Safeguarding Children Board.

List of recommendations

Recommendations	Stakeholder/Responsible Team
Recommendation 1 - That Council work with schools that do not currently have an e-safety strategy to develop this policy, providing advice and guidance and signposting to resources online where appropriate (paragraph 3.6).	Cabinet
Recommendation 2 – That the council and schools provide more regular training for parents and carers to educate them on the risks that young people face, how to manage these and on the safe use of new technologies and discuss what training and awareness raising is required/appropriate, for example, bulletins (paragraph 4.7).	Cabinet/Schools
Recommendation 3 – That schools and the council equip children and their families to remain safe online by signposting to, and providing, information and resources on new and potential risks to young people when online (paragraph 4.7).	Schools
Recommendation 4 – That schools brief new students on the positives and negatives surrounding the use of the internet, for example, profiles on social media sites and potential impact on future employment and educational opportunities, when they sign up to the schools acceptable user agreement (paragraph 4.10).	Cabinet/Schools/MSCB
Recommendation 5 – That Cabinet engage with the council's corporate communications team to consider how best to raise awareness of e-safety issues and how schools and parents can best support young people when online (paragraph 4.10).	Cabinet
Recommendation 6 – That Cabinet explore the use of existing volunteers in libraries being asked to include raising awareness amongst parents and young people on e-safety issues and measures to their role (paragraph 4.10).	Cabinet/MSCB
Recommendation 7 - **That** Cabinet identify schools that are exemplars of good practice in relation to e-safety to provide peer support to schools that require guidance, advice and support on e-safety issues or policy (paragraph 4.10).	Cabinet/Schools
Recommendation 8 – All schools should be encouraged to undertake the e-safety audit developed by the council annually to ensure that their e-safety strategies and measures are effective (paragraph 4.13).	Cabinet
Recommendation 9 – That schools notify the council's MASH team regarding any safeguarding issues concerning e-safety and that the MASH team analyse that data to determine if any vulnerable groups or demographics require additional support to manage online risks. This should feed into schools e-safety policies and action plans (paragraph 6.18).	Cabinet/MSCB
Recommendation 10 – That the council encourage schools to include e-safety on every school council meeting agenda, as a standard item, to enable young people to raise any issues or concerns and for schools to then respond appropriately (paragraph 7.3).	Schools

Recommendation 11 - That Cabinet explore, with schools, the possibility of rolling out existing mechanisms to enable young people to raise concerns anonymously in the first instance to then allow a decision to be taken on how best to respond (paragraph 7.3).	Cabinet/Schools/MSCB
Recommendation 12 – That schools encourage young people to become e-safety champions and to provide support and/or mentor other pupils to provide advice and guidance on any e-safety issues they are encountering (paragraph 7.8)	Cabinet/Schools/MSCB

Final Report of the Task Group

1. Introduction

1.1 The Council's Children and Young People Overview and Scrutiny Panel, at its meeting on 3 July 2014, agreed to establish a Task Group review of online strategies and e-safety in schools. The Panel appointed a small number of Members to the Task Group for a short, very specific review into e-safety that would take 3 months to gather evidence and report accordingly. This length of task group review was being trialled by the Panel to look at how more specific issue and topics might be looked at in greater depth over a shorter time period, to enable the Panel to undertake more work during its annual work programme.

What is e-safety?

1.2 E-Safety is a term which encompasses not only the internet but other ways in which young people communicate using electronic media, for example, smart phones or gaming consoles. It means ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies, without risk to themselves or others.[1]

Rationale

1.3 As noted in the Byron Review (2008), commissioned by the Government as an independent review of the risks children face on the internet, technology offers extraordinary opportunities for all of society.[2]

1.4 It is recognised that technology offers positive opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile. However, pupils are using technology at an ever earlier age and older children are spending more time online. OFSTED noted that children aged 12–15 years are also more likely to mostly use the internet in their bedrooms alone. Furthermore, children are going online via a wider range of devices: Internet access via a PC, laptop or netbook is increasingly being supplemented by access via other devices[3].

1.5 Children's online experiences play a crucial role in many developmental aspects of their lives, such as in exploring their identity and sexuality, building relationships with peers or romantic relationships. [4] However, there is also a generational digital divide between parents and children which means that many parents do not feel

[1] Merton Safeguarding Children Board – Supporting Merton's Young People to stay safe online: An e-Safety Strategy (2014-2015). http://www.merton.gov.uk/merton_e-safety_strategy_2014-15.pdf

[2] The Byron Review (2008) *Safer Children in a Digital World*. http://webarchive.nationalarchives.gov.uk/20101021152907/http://publications.education.gov.uk/eorderingdownload/dcsf-00334-2008.pdf

[3] OFSTED (2014) *Inspecting e-safety in schools*. http://webfronter.com/surreymle/Esafety/other/OFSTED-Inspecting-e-safety-January-2014.pdf

[4] Vandoninck, S; Leen, d'Haenens & Smahel, D. (2014) *Preventative measures – how youngsters avoid online risks*, EU Kids Online www.eukidsonline.net

empowered to manage risks in the digital world in the same way that they do in the 'real' world[5].

1.6 The UK Council for Child Internet Safety have advocated that sound harm-prevention policies for children's internet use be developed in response to potential areas of vulnerability in the broader context of children's lives and that the focus should be on building protective environments for young people[6].

1.7 Technology use and e-safety issues therefore go hand in hand. Many incidents happen beyond the physical geography of the school and yet can impact on pupils or staff. This makes it vitally important that pupils and staff are fully prepared and supported to use these technologies responsibly[7].

1.8 Members expressed concerns about how best to manage children and young people's experiences of online activities and were keen to explore both the positives and negatives of internet use and how they might be managed or promoted to ensure the safe development of young people in the borough.

Purpose

1.9 The overarching aims for the review were established as follows:

- To understand modern day challenges, opportunities and risks online experiences are providing to young people and establish how they are managed and mitigated;
- To ensure that we are safeguarding and promoting the welfare of children when online;
- To enable children to independently use the internet safely and responsibly

1.10 The following Terms of Reference for the Task Group review were agreed:

- To determine what policies and procedures schools have in place to protect children when online;
- To determine if awareness raising is happening in schools with pupils about online safety;
- To determine how online risks are identified and managed in schools;
- To determine how schools can better educate young people to ensure that they maintain a positive online presence;

[5] The Byron Review (2008) *Safer Children in a Digital World*. http://webarchive.nationalarchives.gov.uk/20101021152907/http://publications.education.gov.uk/eorderingdownload/dcsf-00334-2008.pdf

[6] UKCCIS (2013) *What do 17,000 Children in London Tell Us About Online Safety? The London Esafety Report*, www.saferinternet.org.uk

[7] OFSTED (2014) *Inspecting e-safety in schools*. http://webfronter.com/surreymle/Esafety/other/OFSTED-Inspecting-e-safety-January-2014.pdf

- To identify what training staff receive about their online presence and the reputational impact for schools;
- To identify what action is being taken by schools to tackle and prevent online bullying; and
- To determine how the council can better support schools, parents and young people in this area

2. Legal and Inspection framework governing E-safety

2.1 Members reviewed the policy and legislative framework that safeguards children and young people from risk online. E- safety falls within the broad responsibility for safeguarding covered by the following legislation;

- Children's Act 1989, 2004, 2010; and
- The Children and Families Act 2014

2.2 A more detailed outline of additional national policy that schools and councils must adhere to is outlined in Appendix 3. The Byron Review (2008) has also been central to the way that e-safety is legislated for and inspected in schools and other agencies.

2.3 The broadest safeguarding responsibility is integrated into the curriculum and involves parents, starting from key stage two onwards to guide children on basic safety. Schools are therefore held accountable for ensuring a safe online environment for their pupils and educating and raising awareness of risks with children and parents.

2.4 E-safety is governed and inspected in schools by OFSTED and overseen and supported by the Merton Safeguarding Children Board at a local level. OFSTED were made responsible by the Government for evaluating the extent to which schools teach pupils to adopt safe and responsible practices in using new technologies, describing e-safety as the school's ability:

- To protect and educate pupils and staff in their use of technology; and
- To have the appropriate mechanisms to intervene and support any incident, where appropriate

2.5 OFSTED categorise the issues classified within e-safety into three areas of risk: Content, Contact and Conduct (with examples given as to these types of risk below):

Risk Type	Definition	Examples
Content	Being exposed to illegal, inappropriate or harmful material	• exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse • lifestyle websites, for example pro-anorexia/self-harm/suicide sites • Hate sites • content validation: how to check authenticity and accuracy of online content

Contact	Being subjected to harmful online interaction with other users.	• grooming • cyber-bullying in all forms • identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
Conduct	Personal online behaviour that increases the likelihood of, or causes, harm	• privacy issues, including disclosure of personal information • digital footprint and online reputation • health and well-being (amount of time spent online (internet or gaming) • sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images) • copyright (little care or consideration for intellectual property and ownership – such as music and film)

2.6 OFSTED guidance on key features of good and outstanding practice for e-safety is attached as Appendix 4.

2.7 Members noted that both the London Grid for Learning and OFSTED have compiled advice for schools on the measures that they should adopt regarding e-safety at schools, and they should encourage at home, on the safe use of new technologies[8]. These measures can be incorporated in to schools e-safety strategies and cover;

- Provision and responsibility for e-safety being shared by all staff in schools and agreement to act responsibly within and outside the school premises;
- School's expectations for parents being articulated clearly;
- Provision of staff safeguarding training and guidance on how to respond to e-safety incidents/disclosures;
- Schools ensuring that children know how to report e-safety concerns;
- Assemblies, tutorial time, personal, social, health and education lessons, and an age-appropriate curriculum for e-safety to help pupils to become safe and responsible users of new technologies;
- 'Managed' systems to ensure young people have a better knowledge and understanding of how to stay safe, assess and manage risk for themselves;
- Senior leaders, governors, staff and families developing that schools strategy for e-safety together which can be reviewed regularly in

[8] *The safe use of new technologies* (2010), OFSTED.
http://dera.ioe.ac.uk/1098/1/The%20safe%20use%20of%20new%20technologies.pdf

light of technological developments.

3. Local Policy and Safeguarding in Merton

What role does the Local Authority play in safeguarding and e-safety?

3.1 Responsibility for e-safety sits within Merton Anti-bullying and E-safety Operational Group. In line with Merton's e-safety strategy, the council have continued to work with adults, young people and schools to raise awareness of e-safety and cyberbullying. The council have also developed links and worked with:

- Merton Schools Council;
- Head Teachers;
- School Business Managers Forum; and
- Safer Schools Police Team

3.2 Members were pleased to hear that training courses have been developed and now form part of a continuing professional development (CPD) offer delivered in partnership with Sutton and Merton CPD (SAMS). The council, working with the Merton Safeguarding Board (MSCB), have also developed an e-safety audit tool, provide guidance on developing an e-safety strategy and provide IT support to schools.

3.3 The task group heard that other initiatives that the council have supported and jointly delivered with the Merton Safeguarding Children Board include the following:

Internet Matters

3.4 In May a new child internet safety organisation founded by four of the UK's biggest broadband providers, (BT, Sky, TalkTalk and Virgin) to act as a single authoritative resource for child online safety was launched. Internet Matters will encourage the wider technology industry, experts, policy makers and parents to work together to establish world-leading resources. It is intended as a one-stop hub, directing parents to valuable help and advice from the leading experts at organisations and charities in the child internet safety field. The council, working with the MSCB, will aim to promote this initiative in Merton to equip parents with the information they need to make informed decisions.

Digital Footprint

3.5 The enforcement of the Right to be forgotten by the European courts has placed an emphasis on individual privacy and young people's management of their digital footprints, particularly in relation to social media. Awareness raising with all young people will take place to make them aware that:

- Employers regularly trawl social media accounts and it is likely that higher education establishments may also undertake this activity;
- Embarrassing posts may incite bullying; and
- Police in several states of the USA have successfully prosecuted students who possess indecent images on mobile devices including self-generated

sexually explicit selfies. There have been no prosecutions in the UK yet but these images can be construed as illegal.

3.6 The Local Authority also acts as a specialist adviser to support the work of the Merton Safeguarding Children Board. A small team internally support the Board, all with relevant safeguarding experience.

Recommendation 1 - That Council work with schools that do not currently have an e-safety strategy to develop this policy, providing advice and guidance and signposting to resources online where appropriate.

Merton Safeguarding Children Board

3.7 Helping children and young people to stay safe online is a priority for the MSCB. The role of the MSCB is to provide strategic leadership, guidance and inform front line practitioners in order to:

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

3.8 Members considered that as technology changes so new risks appear. The task group also recognised that this can be a source of anxiety to parents and those responsible for the welfare of young people. The MSCB therefore work with a range of partner agencies to keep up with such a rapidly moving scene. The delivery and guidance on e-safety is the responsibility of various groups of professionals and partners that work with schools and in other young people' settings, with the support of, LB Merton Schools ICT Support Team (SMISST), the MSCB and the Anti-Bullying & e-safety working group.

3.9 The MSCB have also developed an e-safety strategy which is designed to provide guidance and support to organisations such as schools, youth providers, voluntary and community sector groups in developing their own responses to the risks to the young people they deal with, and to particularly ensure the most vulnerable are protected from harm.

3.10 The MSCB e-safety strategy covers the following aspects of e-safety:

- Cyber-bullying, including sexual bullying;
- Safe use of social networking;
- Pornography and violent images (accessibility and inappropriate use by young people);
- Grooming by strangers and known contacts, including trusted adults;

- Real time communications including texts, e.g. ‘sexting’, chat rooms, email, instant messaging, video chat etc.;
- Support for parents and carers and their role and responsibilities;
- Support for young people, particularly the more vulnerable; and, ensuring that young people are aware of the risks and do not endanger their ‘online reputation’ by their activity;
- Training for professionals and practitioners; and
- Communications infrastructure (working to developing managed online environments for young people rather than blanket blocking policies).

3.11 The MSCB also supports and encourages in schools and at home the Zip It, Block It, Flag It initiative – the Click Clever, Click Safe Code for children and young people which encourages privacy, blocking nasty messages and enabled issues to be flagged up:

4. How do schools promote and ensure e-safety?

4.1 Schools and other young people’s organisations are encouraged and supported to ensure that e-safety is at the heart of their efforts to safeguard young people, including identification of those who may be vulnerable.

4.2 Members met with both primary and secondary school head teachers to explore the role that schools play in educating, informing young people about e-safety and ensuring they are safe when online. Members heard that schools have strong filters in place. There are email filters for all schools across London and children are taught to zip their personal information, block unknown people, and flag issues of concern.

4.3 The task group learned that the number of incidents of children being at risk in online settings in schools is low. However, heads stated that this does not necessarily mean that e-safety is not an issue as children have access outside of school and within the home. This also means an increased role for parents in safeguarding and monitoring their children’s online activity.

4.4 Schools provide a range of training sessions on e-safety for governors, staff, pupils and parents and have e-safety policies in place which are managed and monitored internally. Also, in many schools IT working parties have been set up which involve the provider, heads and governors to ensure e-safety is effectively monitored.

4.5 Furthermore, schools put in place an acceptable user agreement which all pupils, parents and staff sign up to and deliver e-safety sessions, both as part of the curriculum and during key periods, such as during anti bullying week. School Staff

are trained on e-safety and when interviewed are asked about their online presence (digital footprint) and the potential impact on the reputation of the school.

4.6 Aside from the support received from the council and Merton Safeguarding Children Board, schools utilise a range of resources available online through websites such as CEOP, Childnet, Think you know, NSPCC and London Grid for Learning.

4.7 Schools seek to raise awareness of e-safety issues with parents when they come into school and also provide formal training and awareness raising sessions. Heads informed the task group that getting parents involved is key to ensuring that young people remain safe online and that parental controls are utilised within the home.

Recommendation 2 – That the council and schools provide more regular training for parents and carers to educate them on the risks that young people face, how to manage these and on the safe use of new technologies and discuss what training and awareness raising is required/appropriate, for example, bulletins.

Recommendation 3 – That schools and the council equip children and their families to remain safe online by signposting to, and providing, information and resources on new and potential risks to young people when online.

4.8 Heads emphasised the importance of being mindful that children are sharing more online now and parents don't often realise or acknowledge the extent of their online activity and therefore, do not monitor it as proactively as they perhaps should. Children have Facebook accounts and use social media at a very young age and it can be a challenge to get them to understand the risks of sharing information and views online.

4.9 Heads advised that children need to be made to feel as though they are being equipped with the knowledge to act responsibly, but also that should they access something they deem to be of concern, that they feel comfortable enough raising it with a teacher or parent.

4.10 Heads proposed the following actions needed to be taken to ensure that e-safety messages were reinforced:

- awareness raising at young age with children in schools and with parents;
- encourage use of parental controls in the home;
- encourage internet providers to more widely publicise internet controls available on mobile devices; and
- ensure lines of communication are available for children and parents to raise issues

Recommendation 4 – That schools brief new students on the positives and negatives surrounding the use of the internet, for example, profiles on social media sites and potential impact on future employment and educational opportunities, when they sign up to the schools acceptable user agreement.

Recommendation 5 – That Cabinet engage with the council's corporate communications team to consider how best to raise awareness of e-safety issues and how schools and parents can best support young people when online.

Recommendation 6 – That Cabinet explore the use of existing volunteers in libraries being asked to include raising awareness amongst parents and young people on e-safety issues and measures to their role.

Recommendation 7 - That Cabinet identify schools that are exemplars of good practice in relation to e-safety to provide peer support to schools that require guidance, advice and support on e-safety issues or policy.

How do Governors monitor e-safety and how could they be better supported?

4.9 The task group consulted Governors on their role in ensuring schools had appropriate e-safety measures in place that were robust and effective. Members learned that Governors receive annual training on IT and e-safety from schools and are responsible for approving e-safety and acceptable use policies, as well as ensuring that the correct infrastructure is in place in schools.

4.10 Governors can oversee contracts to IT providers and performance monitor IT and e-safety policies within schools. E-safety is a standard agenda item for some school governing bodies and it is viewed as a whole school issue with all staff and governors receiving training and subsequent refresher training, at appropriate intervals.

4.11 Governors felt confident that schools were doing all they could to support young people to be safe when online. Emphasis was again placed on the need to shift responsibility to parents to be more involved in preventing, managing and educating young people about online risks. The role that the school could play in supporting parents was also highlighted by governors and felt necessary. It was proposed to the task group that this could be achieved through briefings that promote e-safety or be embedded in other information sessions schools provide to parents.

4.12 The task group also heard that communication and education was central to educating young people and parents and that, in some schools, a review of the information made available on the schools website regarding e-safety could be undertaken and the curriculum widened to reinforce e-safety messages, for example, through PSHE and citizenship lessons etc.

4.13 The Governors consulted also required further communication and promotion of some of the tools and support that councils provide to schools to ensure that they are utilising this, for example, the use of an annual e-safety audit as developed by the council, with the MSCB.

Recommendation 8 – All schools should be encouraged to undertake the e-safety audit developed by the council annually to ensure that their e-safety strategies and measures are effective.

4.14 The Governors consulted felt that there was a greater role for schools to play in the following ways:

- To address gender issues in terms of provision of advice, support and guidance on e-safety;
- Provide an online forum to support young people and parents;
- Provide more training for parents;

- To raise awareness and educate young people as early as possible about e-safety and potential risks;
- To provide more in-depth training for governors on safeguarding issues

5. Parental mediation

5.1 Members agreed that parents have a key role to play in managing children's access to online material that may put them at risk or be inappropriate. There is a need to empower parents to support children's online safety from a young age and to ensure that the range of technical tools that can help parents do this, are employed and that parents understand them.

5.2 The task group acknowledge that restricting children's access to harmful and inappropriate material is not just a question of what parents can do to protect children but also what children can do to protect themselves.

5.3 Parents play many roles to a greater or lesser relation in terms of their children's internet use. Some are restrictive, some share of the online experience, some talk about the internet and are involved in their child's online activities (whether in their presence or later). [9]

5.4 A study conducted by the LSE and EU Kids Online found that:

- Parents of children with psychological difficulties feel less able to help;
- Parents who do not use the internet do not feel able to help; and
- Children from minority/discriminated groups have parents who are more likely to doubt their ability to support their child
- Children that have more psychological difficulties have parents who get a little less information on e-safety;
- Parents who speak a minority language at home get a little less information on e-safety[10].

5.6 EU Kids Online also reported that parents with younger children (9-12 years) are a little more likely to get advice from their child's school. As children get older, parents get less safety information from their child's school and more from their child. Parents who don't use the internet, and those whose children use the internet infrequently, are also unsurprisingly less likely to gain safety information from their Internet Service Provider or from dedicated websites.

5.7 Members found that the London E-Safety Report (2013) proposed that parents should be encouraged by schools and the relevant agencies to:

- Talk with their child about what they do online;

[9] Livingstone, S; Gorzig, A &Olafsson, K (2011) *Disadvantaged children and online* risk, EU Kids Online http://eprints.lse.ac.uk/39385

[10] Livingstone, S; Gorzig, A &Olafsson, K (2011) *Disadvantaged children and online risk*, EU Kids Online

- Monitor usage of games, videos and social media and check that they are age appropriate;
- Not assume that there is less risk because children are younger;
- Enable parental controls; and
- Seek help from school staff and online parental support[11]

5.8 Analysis by EU Kids Online and the LSE shows that when parents actively mediate their child's internet use, this too is associated with lower risk and, most importantly, lower harm.[12]

5.9 Active mediation is therefore key and refers to when parents talk to their child about the internet, stay nearby or sit with them while they go online, encourage them to explore the internet, and share online activities with them. These activities, the findings of the EU Kids Online show, tend to reduce children's exposure to online risks without reducing online opportunities, and they also reduce young children's (9-12 years) reports of being upset when they encounter online risks[13].

5.10 However, parents' active mediation of safety (e.g. giving safety or online behaviour advice), and their monitoring of the child's internet use, are generally used after a child has experienced something upsetting online[14]

5.11 Given that children's exposure to online risks decreases the more parents use restrictive mediation, it should be actively encouraged by schools and other relevant agencies. New analysis by EU Kids Online also shows that:

- Parental restrictive mediation leads to a significantly smaller probability of being bothered or upset online (at any age);
- Active mediation of use tends to decrease the experience of harm between 9 and 12 years, though there is no effect for 13 to 16 year olds;
- Active mediation of safety significantly increases being bothered or upset from online risks among 9-10 year olds and 15-16 year olds (with a similar tendency between these ages which is not statistically significant); and
- Monitoring is not significantly linked to feeling bothered or upset at 9-10 or 15-16 but is associated with increased harm between 11-14

6. What risks do young people face online?

6.1 During consultation with young people, teachers and governors, the task group learned that the risks that young people were aware of or had been exposed to in

[11] UKCCIS (2013) *What do 17,000 Children in London Tell Us About Online Safety? The London Esafety Report*, www.saferinternet.org.uk

[12] Duerager, A & Livingstone, S (2012) *How can parents support children's internet safety?* EU Kids Online www.eukidsonline.net

[13] Duerager, A & Livingstone, S (2012) *How can parents support children's internet safety?* EU Kids Online www.eukidsonline.net

[14] Duerager, A & Livingstone, S (2012) *How can parents support children's internet safety?* EU Kids Online www.eukidsonline.net

their use of the internet primarily occurring outside of school systems which has significant safeguards in place. The risks that were apparent resulted from young peoples use of the internet on hand held devices, mobile phones and also in the home. These risks included:

- Online bullying;
- Inappropriate language use and pressure felt when participating in online gaming with people who may not be the same age;
- Being asked to share personal information;
- Receiving or being asked to send inappropriate sexual content, also known as 'sexting. 'Sexting' is defined as: Swapping sexual images by picture message, email, app or social network[15].

6.2 Similarly, research into the risks of internet use and how they are perceived, experienced and managed demonstrates that online experiences can be both positive and negative for young people.

Which children and young people are more vulnerable to online risks?

6.3 The Byron Review (2008) highlighted the need to take into account children's individual strengths and vulnerabilities in their online activity, because the factors that can discriminate a 'beneficial' from a 'harmful' experience online are often individual. The very same content can be useful to a child at a certain point in their life and development and may be equally damaging to another child. The Byron Review (2008) also acknowledges that there are vast individual differences that will impact on a child's experience when online, especially considering the wider context in which they have developed and in which they experience that technology[16].

6.4 The UK Council for Child Internet Safety (UKCCIS) also found that many factors combine to render some children vulnerable to online risk, under particular circumstances, and with diverse consequences[17].

6.5 Members sought to explore which young people were more vulnerable through existing research and reports and through consultation events. The task group met governors, police cadets, teachers, head teachers, safer schools police officers and young people throughout the review. The task group explored vulnerabilities that may be increased by:

- Gender;

[15] London Grid for Learning (2013) 1 Minute Guide - 'Sexting' http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx?tab=4

[16] The Byron Review (2008) *Safer Children in a Digital World*. http://webarchive.nationalarchives.gov.uk/20101021152907/http://publications.education.gov.uk/eorderingdownload/dcsf-00334-2008.pdf

[17] UKCCIS (2013) *What do 17,000 Children in London Tell Us About Online Safety? The London Esafety Report*, www.saferinternet.org.uk

- Disability;
- Special educational needs; and
- Socio economic background

6.6 The Task Group utilised the findings of an EU Kids Online study of online bullying and disadvantaged children. They found that online bullies and those being bullied online are those children who are mostly also vulnerable offline. This includes children who have psychological difficulties, are socially excluded; engage in unhealthy attention seeking behaviours or are in some way or another, members of a vulnerable group. [18] Among those involved in online bullying, girls, younger children and those from a low socio-demographic background report more often being victims of bullying than those with a higher socio-demographic background.[19]

6.7 The Task Group also considered the findings of three Youth Internet Surveys that were undertaken over a 10 year period to examine the online bullying experiences of young people. Online bullying or cyber bullying is when a person or a group of people uses online digital technology to threaten, tease, harass, upset or humiliate someone else. In many cases, a single act can go viral resulting in a feeling of 'repeated' bullying as wider audiences are involved. The victim's privacy can also be invaded at all times[20].

6.8 Members learned and expressed concerns that cyber bullying can cause young people to feel humiliated, to feel isolated from friends, to play truant or self harm and in more server cases, commit suicide. This highlights the significance of taking the appropriate measures to ensure that young people are safe online and feel comfortable and confident enough to report any issues, concerns or experiences.

6.9 The surveys undertaken specifically examined victimisation and perpetration behaviours. The data collected sought to establish how these behaviours changed across the three survey points and whether demographics and internet use patterns had changed for all youth internet users, compared with those that had experienced online bullying.

6.10 Members considered the findings from the Surveys which were as follows:

- Those experiencing online bullying increased to 11% in 2010;
- More serious online bullying or repeated incidents were only experienced by 5% of young people;
- The rate of female versus male victims of online bullying changed significantly throughout the course of the survey;
- 13-15 year olds make up the largest proportion of young people bullied in all three cohorts;
- The percentage of girls engaging in online bullying increased to 48% by 2010;

[18] Gorzig, A (2011) *Who bullies and who is bullied online? : a study of 9-16 year old internet users in 25 European countries*. EU Kids Online www.eukidsonline.net

[19] Gorzig, A (2011) *Who bullies and who is bullied online? : a study of 9-16 year old internet users in 25 European countries*. EU Kids Online www.eukidsonline.net

[20] London Grid for Learning (2013) *1 Minute Guide – Cyberbullying*. http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx?tab=4

- Disclosure to school staff increased to 12% by 2010[21]

6.11 When consulting with young people about when they felt that online activities could turn into problematic or harmful situations, the survey identified the following risks, which have also been noted in research undertaken by EU kids Online study in 2014. The types of risk identified related to:

- online bullying;
- unwelcome contact from strangers;
- misuse of personal information;
- issues related to sexual content or communication;
- commercial content[22]

6.12 The prevalence of social networking sites in young people's lives ultimately plays a role in increasing the occurrence of the risks identified above. However, young people will not necessarily stop engaging with these sites as they are a means by which to maintain friendships and to be culturally aware[23]. Social networking has become one of the most popular activities online. However, whilst age restrictions apply, these are only partially effective. By combining chat, messaging, photo albums and blogging, social network sites integrate online activities more seamlessly than ever. This offers children many opportunities but also many risks. [24]

6.13 Members acknowledged that, given the possible risks, as well as the many opportunities afforded by social networking, and since much usage occurs away from adult supervision, children's own digital skills are crucial. This includes children's ability to use the safety features embedded in these sites. [25]

6.14 The consultation undertaken by the Group found that young people have experienced:

- unwelcome contact on social networking sites;
- abusive language when online gaming;
- pressure to engage in 'sexting' (sending images or messages of an explicit nature and sexual content); and
- Bullying through social media

6.15 Members also consulted young people and recent research to explore the impact that gender had on how vulnerable young people were to online risks. The task group

[21] UKCCIS (2013) *Online Harrasment in Context: Trends from Three Youth Internet Safety Surveys (2000-2010)* www.education.gov.uk/ukccis/

[22] Vandoninck, S; Leen, d'Haenens & Smahel, D. (2014) *Preventative measures – how youngsters avoid online risks*, EU Kids Online www.eukidsonline.net

[23] Vandoninck, S; Leen, d'Haenens & Smahel, D. (2014) *Preventative measures – how youngsters avoid online risks*, EU Kids Online www.eukidsonline.net

[24] Livingston, S, Olafsson, K & Staksrud, E (2011) *Social Networking, age and privacy*, EU Kids Online www.eukidsonline.net

[25] Livingston, S, Olafsson, K & Staksrud, E (2011) *Social Networking, age and privacy*, EU Kids Online www.eukidsonline.net

found that girls and boys engage and cope with what they encounter online slightly differently[26]. However, many of the young people engaged noted that their ability to cope with such incidents, respond and determine whether to report these was down to individual resilience and peer support/network in school, not gender.

6.16 Young people stated that boys and girls were both likely to report incidents and be victims of online bullying or have received inappropriate sexual messages or images on their phones/social networking sites.

6.17 Members also raised questions regarding the ability of disadvantaged children to cope with online risks. EU Kids Online and the LSE considered the educational/economic; psychological and social disadvantage that young people faced and the potentially negative impact these factors might have when engaging in online activities.[27]

6.18 It was reported by EU Kids Online that when it comes to being bullied online:

- Girls are more likely to tell than boys, often a friend. Boys will still report incidents however;
- Younger children are more likely to tell a parent or sibling when they are upset because they are being bullied online, while older teenagers are least likely to tell a teacher;
- Parents who are aware of a child having been upset by something online are, unsurprisingly, more likely to have a child who tells their parents what happened to them; and
- Those from discriminated against groups or who speak a minority language at home are much more likely to tell someone than are other children, especially a parent. [28]

Recommendation 9 – That schools notify the council's MASH team regarding any safeguarding issues concerning e-safety and that the MASH team analyse that data to determine if any vulnerable groups or demographics require additional support to manage online risks. This should feed into schools e-safety policies and action plans.

7. Young peoples knowledge of effective preventative measures

7.1 The task group agreed that digital literacy plays a vital role in children's use of the internet, both resulting from and further stimulating the range and depth of children's online activities. It is widely hoped that, as children become more digitally literate,

[26] Livingstone, S; Gorzig, A &Olafsson, K (2011) *Disadvantaged children and online risk*, EU Kids Online http://eprints.lse.ac.uk/39385

[27] Livingstone, S; Gorzig, A &Olafsson, K (2011) *Disadvantaged children and online risk*, EU Kids Online http://eprints.lse.ac.uk/39385

[28] Livingstone, S; Gorzig, A &Olafsson, K (2011) *Disadvantaged children and online risk*, EU Kids Online http://eprints.lse.ac.uk/39385

the more they will gain from the internet while also being better prepared to avoid or cope with online risks.[29]

7.2 The task group learned that young people are less fearful of online risks when they feel they are able to handle them or have appropriate mechanisms that they feel comfortable accessing to raise these issues. Predominantly, young people turn to their peers for support and would talk to a teacher secondly and a parent last. Young people however, do need to know where they can go for confidential advice and support.

7.2 The issue of embarrassment and shame was highlighted by some young people when asked why parents are not approached about online risks and incidents. Many young people are concerned that schools will inform parents of any issues which they may prefer them not to know about.

7.3 School mechanisms, such as the Youth That Care team (YTC), a service managed by pupils within a school to provide support and advice, are not used often. This is because young people have concerns about confidentiality and issues being reported to parents. It was also suggested that school councils do not spend enough time looking at e-safety and considering issues. Young people engaged stated that teachers need to ensure that they listen and implement recommendations from young people when they report e-safety concerns.

Recommendation 10 – That the council encourage schools to include e-safety on every school council meeting agenda, as a standard item, to enable young people to raise any issues or concerns and for schools to then respond appropriately.

Recommendation 11 - That Cabinet explore, with schools, the possibility of rolling out existing mechanisms to enable young people to raise concerns anonymously in the first instance to then allow a decision to be taken on how best to respond.

7.4 Young people consulted as part of this review also proposed that schools block internet access and remove phones from pupils; others suggested that moderate internet access should be allowed on hand held devices/mobile phones in schools.

7.5 The following preventative strategies adopted by young people were identified and captured into the following categories by EU Kids Online:

- Employ problem solving strategies such as speaking to peers to determine how to respond to an incident;
- Plan and reflect upon how to deal with potential risks;
- Seek information to increase knowledge or skills about online safety;
- Seek support to obtain advice or aid that should help prevent an incident[30]

[29] Livingstone, S; Gorzig, A &Olafsson, K (2011) *Disadvantaged children and online risk*, EU Kids Online http://eprints.lse.ac.uk/39385

[30] Vandoninck, S; Leen, d'Haenens & Smahel, D. (2014) *Preventative measures – how youngsters avoid online risks*, EU Kids Online www.eukidsonline.net

7.6 The strategies employed by the young people consulted by the task group fit within those identified by EU Kids Online which are as follows:

Instrumental action – deleting, unfriending or blocking certain people;

Self monitoring – limiting their online activities;

Behavioural avoidance – in situations of unpleasant sexual issues, children do not perceive limiting their online activities as useful. As EU Kids Online have noted, young people avoid unpleasant sexual content or communication by turning away from the situation or making sure one does not get involved. [31]

7.7 Young people also highlighted that they should be involved sooner in meeting with other children and other young people to talk to them about online safety. They noted that young people only tend to hear about extreme experience of e-safety such as when someone is murdered by a stranger or a young person commits suicide because of cyber bullying. There tends to be less information about peoples regular experiences.

7.8 The task group feel that the best people to support young people to be safe online are other young people; as they understand the risks and issues, and know what young people are actually doing online. A forum or mechanism for young people to engage with other young people should be explored.

Recommendation 12 – That schools encourage young people to become e-safety champions and to provide support and/or mentor other pupils to provide advice and guidance on any e-safety issues they are encountering.

[31] Vandoninck, S; Leen, d'Haenens & Smahel, D. (2014) *Preventative measures – how youngsters avoid online risks*, EU Kids Online www.eukidsonline.net

5. Concluding Remarks

5.1 The task group were very clear at the outset of this review that children have the right to protection and safety online and that the role of safeguarding agencies, the local authority, schools and parents should be further strengthened and effective to achieve this.

5.2 The task group also acknowledge that no amount of effort to reduce potential risks to children when online will eliminate those risks completely. The internet cannot be made entirely safe. New means of internet access are also less open to adult supervision and technical solutions are one element of a broader strategy on e safety [32].

5.3 We must therefore work in partnership to build children's *resilience* to the material to which they may be exposed so that they have the confidence and skills to navigate these risks. [33] Children and young people need to be encouraged to develop self governing behaviour and to take greater responsibility. We need to focus on how kids manage their safety in their own personal space and provide guidance to children as both victims and potential perpetrators.

5.4 When awareness raising, the council, schools, MSCB and parents should emphasise empowerment rather than restriction, and appropriate, responsible behaviour with regard to technology use. Nevertheless, young people still need to know where to go to report any issues or concerns. This is of the utmost importance.

5.5 The task group also felt that communicating online opportunities and positive experiences should be encouraged. Schools should continue to provide educational support for increasing digital literacy and support the mitigation of digital exclusion amongst vulnerable groups. Inequalities in digital skills persist in terms of socio-economic background, age and to a lesser extent and gender. Efforts to overcome these are needed.

5.6 A careful balancing act is therefore required in our approach to e-safety across schools, the MSCB and by parents and carers at home. There must be recognition of both the risks and opportunities of online activity and that children's online experiences 'in the round' are vital.

5.7 The recommendations of the task group seek to highlight the significance of:

- Appropriate, sensitive responses to online and offline bullying;
- On-going dialogue about new risks young people are experiencing;
- Addressing risks associated with peer to peer conduct;
- Informing parents and young people on effective coping strategies;

[32] O'Neill, B, Livingstone, S & McLaughlin, S (2011) *Final recommendations for policy, methodology and rese*arch, EU Kids Online. http://eprints.lse.ac.uk/39410/

[33] The Byron Review (2008) *Safer Children in a Digital World*. http://webarchive.nationalarchives.gov.uk/20101021152907/http://publications.education.gov.uk/eorderingdownload/dcsf-00334-2008.pdf

- Enhancing the role that schools and governors ply in monitoring and managing e-safety in schools; and
- Practical mediation skills for parents as part of the overall effort to build awareness of risks and safety online.

6. What Happens Next?

6.1 This report will be presented to the Children and Young People Overview and Scrutiny Panel meeting on 1 July 2015 for the Panel's approval.

6.2 The Panel will then send the report to the Council's Cabinet meeting in September 2015 for discussion and to seek agreement to the recommendations presented.

6.3 The Cabinet will be asked to provide a formal Executive Response and Action Plan to the Panel within two months of the submission of the report to its meeting in November 2015. The Cabinet will be asked to respond to each of the task group's recommendations, setting out whether the recommendation is accepted and how and when it will be implemented. If the Cabinet is unable to support and implement some of the recommendations, then it is expected that clearly stated reasons would be provided for each.

6.4 The lead Cabinet Member (or officer to whom this work is delegated) should ensure that other organisations, to which recommendations have been directed, are contacted and that their response to those recommendations is included in the Executive Response and Action Plan.

6.5 The Panel will seek a further report six months after the Cabinet response has been received, giving an update on progress with implementation of the recommendations.

Appendix 1

Whom we spoke to

External Organisations:

Gary Hipple – Governor, Ursuline High School
Tim Mann – Met Police
Police Cadets: Shiva Hetheecharan, Shane Dye, Sam Watson, Georgia Milner

Members of:
Scouts
Girl Guides
Children in Care council
Youth Parliament

Primary Heads Group

Secondary Heads Group

Keith Makin – Chair of Merton Safeguarding Children Board

Officers:
Paul Ballatt
Lee Hopkins
Derek Crabtree
Caroline Land
Bev Selway

Cabinet Members:
Councillor Martin Whelton
Councillor Maxi Martin

Appendix 2
Equality Impact Assessment (EqIA) template
Initial Screening

This form should be completed in line with the Equality Impact Assessment guidance available on the intranet The blue text below is included to help those completing the template and should be overwritten.

EqIA completed by: (Give name and job title)	Rebecca Redman, Scrutiny Officer
EqIA to be signed off by: (Give name and job title)	*Julia Regan, Head of Democracy Services*
Department/ Division	Corporate Services, Democracy Services
Team	The Scrutiny Team
EqIA completed on:	23 June 2015
Date of Challenge Review (if you have one):	N/A
Date review of this EqIA is due (no later than 3 years from date of completion):	TBC

What are you assessing? (Tick as appropriate)

- ✓ ***Policy:*** *A policy is an adopted approach by the Council to a specific issue or position, usually in the long term. It provides a set of ideas or principles that together form a framework for decision making and implementation.[1] A policy may be written or unwritten, formal or informal. For example, the Corporate Equality Scheme.*
- ☐ ***Strategy:*** *A strategy sets out the activities and actions that have been identified as most likely and cost-effective to achieve the aims and objectives of a council policy e.g. the Consultation Strategy.*
- ☐ ***Procedure:*** *A procedure sets out the way in which practices and actions are to be undertaken at an individual level in order to achieve the policy in local situations, for example using a flow chart approach. Procedures also outline who will take responsibility on a day to day basis for decisions in the implementation of the policy.[2] For example, this procedure for carrying out an EqIA.*
- ☐ ***Function:*** *A function is an action or activity that the Council is required to carry out for example emergency planning arrangements.*
- ✓ ***Service:*** *A service is a facility or provision made by the Council for its residents or staff for example the Library service or Translation service.*

1. Title of policy, strategy, procedure, function or service

   Support for e-safety advice and guidance to schools, role of police and safer schools police officers, role of schools in relation to ensuring e-safety policies are in place and issues managed, as well as awareness raising with governors, parents and pupils./

2. For functions or services only: Does a third party or contractor provide the function or service? If so, who?

Yes. Partner agencies within Merton Safeguarding Children Board.

3. Who is the policy, strategy, procedure, function or service intended to benefit?

Schools, parents, governors, children and young people

4. Who else might be affected?

-

5. What is known about the demographic make up of the people you have included in your answers to questions 4 and 5?

Profiles of children and young people within Merton schools held by the relevant team within CSF.

6. Have you already consulted on this policy, strategy, procedure, function or service? If so, how?

Consultation undertaken throughout task group review.

[1] See the Council's Policy Handbook http://intranet/policy_handbook_final_agreed_nov_07-2.doc
[2] As above

7. How will you measure the success of your policy, strategy, procedure, function or service?

Performance monitor delivery of the agreed recommendations through the executive response and action plan and going forward on a six monthly basis at Panel meetings. A Member Champion will also be appointed.

8. How often will the policy, strategy, procedure, function or service be reviewed?

See above.

9. When will the policy, strategy, procedure, function or service next be reviewed?

November 2015 when the Executive Response and Action Plan is received by the Scrutiny Panel.

10. Please complete the following table and give reasons for where:
    (a) The policy function or service could have a positive impact on any of the equality groups.
    (b) The policy function or service could have a potential negative impact on any of the equality groups.

Think about where there is evidence that different groups have different needs, experiences, concerns or priorities in relation to this policy, strategy, procedure, function or service.

Equality group	**Positive impact**		**Potential negative impact**		Reason
	Yes	No	Yes	No	
Gender (inc. Transgender)	✓			✓	All of the recommendations seek to both support and empower young people and their parents to manage the child's online activity and associated risks in a supportive environment both in school and at home. Mechanisms are recommended and strengthened in these recommendations to ensure online risks are well managed and responded to and that parental awareness and skills are raised and developed to deal with these risks.
Race/ Ethnicity/ Nationality	✓			✓	
Disability	✓			✓	
Age	✓			✓	
Sexual orientation	✓			✓	
Religion/ belief	✓			✓	
Socio-economic status	✓			✓	

11. Did you have sufficient data to help you answer the above questions?

✓ **Yes**

☐ **No**

If there is a potential negative impact on one or more groups, or there was insufficient data to help you answer the above questions, you should complete a full EqIA

12. Is a full Impact Assessment required?

☐ **Yes**

✓ **No**

EqIA signed off by:	Julia Regan, Head of Democracy Services.
Signature:	
Date:	

Appendix 3

The Legal Framework surrounding e-safety

This section is designed to inform users of legal issues relevant to the use of electronic communications. For older students, discussion of current legislation could be incorporated into the curriculum as part of ICT, PSHE or Citizenship. It might also be useful to make reference to this when dealing with e-safety infringements to reinforce the seriousness of issues arising.

Communications Act (2003)
(section127)

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 committed as soon as the message has been sent: there is no need to prove any intent or purpose.

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).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

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.

Data Protection Act (1998)

The Act 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.

Education Act (2011), sections 2 to 4, provides further clarification on statutory staff powers to discipline pupils for inappropriate behaviour or not for following instructions, both on and off school premises. Further details for Free schools can be found in section 36 and for Academies in Part 6, sections 55 to 65.

Education and Inspections Act 2006, sections 90 and 91, provide statutory powers for staff to discipline pupils for inappropriate behaviour or for not following instructions, both on and off school premises. **Section 94** also gives schools the power to confiscate items from pupils as a disciplinary penalty. These powers may be particularly important when dealing with e-safety issues: online bullying may take place both inside and outside school, and this legislation gives schools the legal power to intervene should incidents occur. It also gives teachers the power to confiscate mobile phones, and other personal devices, if they suspect that they are being used to compromise the well-being and safety of others.

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.

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

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.

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 Equality Act
(2010)

The Equality Act 2010 provides a single, consolidated source of discrimination law, all the types of discrimination that are unlawful. It defines that schools cannot discriminate against pupils because of their sex, race, disability, religion or belief and orientation. Protection is now extended to pupils who are pregnant or undergoing reassignment. However, schools that are already complying with the law should there be major differences in what they need to do.

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 abuse based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act
(2000)
The Regulation of Investigatory Powers Act 2000 (RIP) 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.

Sexual Offences Act
(2003)

A 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) and then intentionally meet them or travel with intent 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. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document, which is available from the Home Office website (www.homeoffice.gov.uk/documents/children-safer-fr-sex-crime?view=Binary).

More information about the 2003 Act can be found at
www.teachernet.gov.uk

Appendix 4

OFSTED Guidance on key features of good and outstanding practice for e-safety

Whole school consistent approach	All teaching and non-teaching staff can recognise and are aware of e-safety issues. High quality leadership and management make e-safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-Safety Mark). A high priority given to training in e-safety, extending expertise widely and building internal capacity. The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	School-based online reporting processes that are clearly understood by the whole school, allowing the pupils to report issues to nominated staff, for example SHARP. Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.
Staff	All teaching and non-teaching staff receive regular and up-to-date training. At least one staff member has accredited training, for example CEOP, EPICT.
Policies	Rigorous e-safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors. The e-safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. The e-safety policy should incorporate an Acceptable Usage Policy that is signed by pupils and/or parents as well as all staff and respected by all
Education	A progressive curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes.
Infrastructure	Recognised Internet Service Provider or RBC together with age/maturity related filtering that is actively monitored.
Monitoring and Evaluation	Risk assessment taken seriously and used to good effect in promoting e-safety. Using data effectively to assess the impact of e-safety practice and how this informs strategy.
Management of Personal Data	The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

This page is intentionally left blank