OXFORDSHIRE COUNTY COUNCIL

E-safety and Cyberbullying Toolkit – January 2015
This toolkit provides information and resources for promoting e-safety of children and young people and preventing and tackling cyberbullying.

Contents:

E-safety Overview Checklist – This provides a quick overview of whether you have measures in place to ensure that you are safeguarding children including e-safety as outlined in the Ofsted framework. This checklist is based on the South West Grid for Learning 360 degrees safe tool http://www.360safe.org.uk/Home. Please refer to the tool for more information. We would recommend that all Oxfordshire schools sign up for the 360 degrees safe tool and that all youth settings sign up for the http://www.onlinecompass.org.uk/

Policy and Leadership

1. Who is responsible for E-safety? Do you have an E-safety Co-ordinator, an active e-safety committee including all stake holders and are governors involved in developing policy and monitoring of incidents?
2. Do you have a comprehensive e-safety policy?
3. Are Acceptable User Policies in place, appropriately differentiated and signed annually by all stake holders?
4. Is E-safety part of self-evaluation and linked to other relevant policies e.g. behaviour policy, Anti-Bullying policy, ICT policies, safeguarding etc.
5. Are their sanctions that are understood by all, imposed and cover out of school bullying?
6. Are their clear systems for reporting understood by all?
7. Are their clear policies in relation to mobile phones, digital images, use of communication technologies (e-mail, chat, blogs, etc.) school website/learning platform?
8. Are there clear protocols, professional standards in place regarding communication of staff with other members of schools and wider community?

Infrastructure

1. Are their clear policies in relation to passwords and are passwords secure?
2. Is schools internet service provided by a recognised ISP with filters and monitoring?
3. Do school systems meet technical security requirements?
4. Are their clear policies in place regarding personal data understood by all stakeholders?

Education

1. Is there a planned e-safety education embedded in all aspects of the curriculum including protecting vulnerable learners? Does it involve young people as peer educators?
2. Are pupils taught about information literacy including developing skills for safe and discriminating online behaviour?
3. Are young people's skills recognised and are they involved in e-safety education?
4. Is there a planned programme of formal e-safety staff training that is regularly reviewed and integral to child protection/safeguarding training?
5. Is e-safety awareness training provided for Governors?
6. Are parent/carers provided with opportunities for training, information and know who to contact if concerned?
7. Does the school provide opportunities for members of the wider community to gain information and understanding about e-safety?

Standards and Inspection

1. Is there monitoring and reporting of e-safety incidents?
2. Is e-safety policy and practice monitored and reviewed?

Local data on e-safety and cyberbullying
Local data indicates that cyberbullying is an issue for both primary and secondary schools. From 765 10 -11 year olds from 14 primary schools who took part in the Oxfordshire Cybersurvey 2014, results indicates that 70% of 10 and 11 year olds have a computer or lap top they can use alone, 24% have a smart phone on which they can access the internet and 16% have a facebook account. 28% had received some kind of abusive or unpleasant message on line (including 6% who had a message from a stranger suggesting they meet up). 17% answered no to “I have never been cyberbullied”. This data is in line with national statistics and highlights the importance of tackling these issues both in primary and secondary schools.

E-safety resources and links
Oxfordshire’s Internet Safety and Cyberbullying web pages provide comprehensive guidance, information and resources for working with children and young people which are regularly updated. http://schools.oxfordshire.gov.uk/cms/content/internet-safety-and-cyberbullying
If you would like to receive further information and updates via the Anti-Bullying network please contact jo.brown@oxfordshire.gov.uk

Policy and Leadership
For developing your E-safety policies we recommend South West Grid for Learning model policies for schools http://www.swgfl.org.uk/Staying-Safe/For-Schools/Policies The SWGfL Template Policies consists of an overall E-Safety Policy and a series of appendices with more detailed template policies and forms. They can also be found embedded in the links and resources section of the 360 degree e-safety self-review tool.

For further information about what should be included in your Anti-Bullying Policy with reference to cyberbullying please see cyberbullying section below.

Professional Standards please follow http://schools.oxfordshire.gov.uk/cms/content/safeguarding to find Simple guidance for staff in education settings on the use of social network sites (pdf format, 92Kb) and please see also Childnet Internationals’ “Using technology guide” http://www.childnet.com/teachers-and-professionals/for-you-as-a-professional/using-technology

Education
To develop a planned e-safety curriculum please see the SWGfL Digital Literacy curriculum - www.swgfl.org.uk/digitalliteracy   Developed from USA Common Sense Media programme SWGfL has produced a series of documents that signpost schools to the relevant Common Sense Media lesson plan, resources and to additional relevant materials from the UK, Europe and elsewhere. The resources cover key stages 1 – 5.

Other resources are available on http://www.childnet.com/resources and http://www.ceop.police.uk/ which links to http://www.thinkuknow.co.uk/ internet safety resources. Our own web pages also include a range of resources.
http://schools.oxfordshire.gov.uk/cms/content/internet-safety-and-cyberbullying

Involving young people
For supporting the involvement of young people consider attending Oxfordshire Anti-Bullying Ambassador training which includes training on cyberbullying and promotes peer education and young people’s involvement in tackling bullying and promoting safer internet use. For further information please search for Anti-Bullying Ambassadors and also internet safety on Oxfordshire’s youth website www.oxme.inf . To find out dates of next ambassador training please contact jo.brown@oxfordshire.gov.uk

Oxfordshire Cybersafety Survey

To support and involve young people and find out about the important issues that need to be addressed in your school please take part in the Oxfordshire Cybersafety survey. Your school or setting can be provided with an individual link. The survey takes about 10 minutes to complete and you will then be provided with a PDF summary of your results including the responses to open ended questions. Please view the sample links for further information and contact jo.brown@oxfordshire.gov.uk if you would like to take part.
Primary Sample 2014
Secondary Sample 2014

Standards and Inspection

The SWgFL model policies includes a "Responding to incidents of misuse flowchart" which can be accessed with the other model policies here http://www.swgfl.org.uk/Staying-Safe/For-Schools/Policies The 'Sexting' in Schools: advice and support around self-generated images. What to do and how to handle it.(see sexting section below) includes a checklist for managing a sexting incident (see annex 1 of the guidance). NB If this is a safeguarding issue please contact the Multi Agency Safeguarding Hub https://www.oxfordshire.gov.uk/cms/content/safeguarding-hub

For further advice on dealing with incidents please contact the Safer Internet Professional Online Helpline for staff. http://www.saferinternet.org.uk/helpline **0844 381 4772** The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. The helpline aims to resolve issues professionals face about themselves, such as protecting professional identity and reputation, as well as young people in relation to online safety.

Cyberbullying

Cyberbullying has similarities to traditional bullying and much of the guidance and advice in relation to bullying applies. There are some differences which can be summarised as follows:

- Bullying can happen 24/7 making it difficult to escape.
- The audience for bullying is potentially much larger increasing the impact
- Cyberbullying incidents can quickly escalate making them difficult to contain
- Anonymity and being one step removed makes it easier for the bystander to join in.
- Anonymity also increases the impact on those being bullied as they can't be sure who is responsible.
- There is a general lack of awareness that behaviour is cyberbullying and young people tend to underestimate the impact of their behaviour.
- Unlike traditional forms of bullying, evidence is readily available and should be preserved.

Guidance

The coalition government has recently issued (November 2014) advice for teachers and schools staff on cyberbullying. This can be accessed, along with advice for parent/carers on cyberbullying and general guidance on bullying by following the link below.
https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Please see Oxfordshire's Anti-Bullying Web Pages for resources, templates and guidance for dealing with bullying all of which are relevant to dealing with cyberbullying.
http://schools.oxfordshire.gov.uk/cms/content/policy-and-guidance

The Legal framework in relation to schools

As outlined in DfE guidance "Preventing and Tackling Bullying" (updated November 2014). teachers have the power to discipline pupils for misbehaving outside the school premises "to such an extent as is reasonable" and the recent government Cyberbullying guidance states that "All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school". The guidance also states that "*where bullying outside school is reported to school staff, it should be investigated and acted on"*.

Section 89(5) of the **Education and Inspections Act 2006** gives head teachers the power to regulate pupils' conduct when they are not on school premises and are not under the lawful control or charge of a member of school staff".

Schools should therefore review the local circumstances and consider putting into place this power to intervene in out of school issues which have the potential to impact on the behaviour, discipline and welfare of the student body as a whole.

Other professionals working with parents/carers will need to make them aware of schools powers in this area if relevant.

Cyberbullying and your Anti-Bullying Policy

Schools are advised to make it clear in their Anti-Bullying policy when they will be exercising the power to discipline pupils off the school site and to give examples of when this would be likely to happen. This will ensure that both parent/carers and young people are fully aware of what behaviour is unacceptable and when schools are likely to intervene.

It is therefore advisable to quote the section of the law as follows: The Education and Inspections Act 2006 gives Head teachers the power "to such an extent as is reasonable to regulate the behaviour of pupils when they are off the school site". For example if members of the school community are involved in cyberbullying a fellow student or staff member the school will exercise this power in order to safeguard the well-being or student or staff member.

Provide examples like:

- Cyberbullying via Social Networking Sites e.g. malicious message on somebody's or profile, creation of a fake profile.
- Filming on mobile phones and passing on inappropriate material or joining in with this behaviour even if you weren't the original author.

For further advice about what should be in your Anti-Bullying policy please see Anti-bullying policy checklist (pdf format, 162KB)

Other settings

Other youth settings may feel it appropriate to refer to schools if they become aware of bullying relating to members of the same school community. They should also have their own Anti-Bullying policy in place which makes it clear what behaviour is unacceptable and what action will be taken. This could include reporting the matter to the police if appropriate.

Sexting

The following resources are useful for preventing and dealing with sexting which has E-safety implications and is usually linked to cyberbullying.

For younger children: NSPCC Share Aware campaign www.nspcc.org.uk/ShareAware including advice about how to keep safe online

www.parentsprotect.co.uk have produced a very useful guide for dealing with sexting in schools

'Sexting' in Schools: advice and support around self-generated images. what to do and how to handle it. It includes practical advice for teaching staff about what to do if sexting happens in school, highlights the steps that need to be taken, and offers examples of best practice through case studies. It also gives an overview of the problem and offers an insight into the research and categorisation of sexting incidents. It highlights some activities that schools can do to highlight the issues and develop a 'whole school' approach.

http://www.swgfl.org.uk/sextinghelp South West Grid for Learning have produced So You Got Naked Online a resource that offers children, young people and parents advice and strategies to support the issues resulting from sexting incidents.

CEOP think u know resources includes the video “Exposed” which deals specifically with the issue of sexting http://www.thinkuknow.co.uk/

http://www.parentsprotect.co.uk/internet_safety_links.htm Parent Protects comprehensive links in relation to internet safety and cyberbullying.

Cyberbullying and Special Educational Needs

Some groups of children are potentially more vulnerable and more at risk than others when using ICT. These can include children with emotional or behavioural difficulties, learning difficulties, and other complex needs, as well as those whose English is an additional language, and looked after children. They may be particularly vulnerable to e-safety risks. For example:

- Some children and young people are more likely to make literal interpretations of content which will affect how they respond for example, those who are hearing impaired, those with Autism Spectrum Disorder and/or those who have language and communication difficulties.
- Some children may not understand much of the terminology due to language delays or disorders.
- Some children with complex needs do not understand the concept of friendship, and therefore trust everyone implicitly. They do not know how to make judgments about what is safe information to share. This leads to confusion about why you should not trust others on the internet.
- There is also growing concern around cyberbullying. We need to remember that some children with SEN or disabilities may be vulnerable to being bullied through the internet, or not recognise that they are being bullied.
- In addition, some children may not appreciate how their own online behaviour may be seen by someone else as bullying.
- Further advice regarding individual young people supported by the SENSS Communication and Interaction Service/ Sensory , Physical Difficulties /Complex Needs teams, including strategies, how to present information and working with young people 1:1 can be obtained from the Special Educational Needs Support Services (SENSS) on 01865 456702 or by contacting the Advisory Teacher involved.

Useful links and resources
http://www.childnet.com/resources/know-it-all-for-teachers-sen provides information and guidance relating to cyberbullying and Special Educational Needs and also provides resources that may be useful

Cerebra have produced a guide “Learning Disabilities, Autism and Internet Safety. A Parents' Guide” which can be accessed in the parent guide section of their website www.cerebra.org.uk (get information/guides for parents and professionals)

Advice from the National Deaf Children's Society on dealing with cyberbullying including an excellent film on internet safety and cyberbullying with signing and sub-titles is available on the following link.
http://youngpeople.ndcsbuzz.org.uk/topics/rss/ref:N4CE1360867E90/

http://anti-bullyingalliance.org.uk/send-resources/cyberbullying-send/send-and-cyberbullying-guidance-for-professionals/ . Guidance for schools and children's workforce for tackling cyberbullying for children and young people with Special Needs and Disabilities.

http://www.anti-bullyingalliance.org.uk/send-programme/. Anti-Bullying Alliance SEND Information hub including resources and links and access to online training programme.

Preventing Cyberbullying Checklist

NB: Consider having a specialist member/s of staff who has expertise in responding to bullying and some technical knowledge in internet and mobile phone use. This could be the person who is your Anti-Bullying co-ordinator or safeguarding lead. This person should develop an action plan to cover the following:

- Ensuring that you have good measures in place to promote the e-safety of children, young people and staff will also protect them from cyberbullying.
- Ensure that curriculum content includes raising awareness about cyberbullying, impact and how to deal with it. For older young people, this should include information about the implications of sexting and the possible consequences for those who send or receive decent images of young people who are under 18 (see E-safety section on sexting)
- Having a clear policy which has been developed involving all stakeholders (young people, adults, parents/carers) that defines cyberbullying, explains what behaviour is unacceptable and makes it clear how to report. (see E-safety policy section)
- Providing detailed advice on how to respond if you think you have been cyberbullied or know someone else who has. Further information in the young people section below
- Having good systems for reporting that are understood by young people, all staff and parents/carers.
- Having student friendly and parent friendly leaflets ideally developed by students
- Raising awareness with staff in terms of how to respond and support young people and also how to protect themselves from potential cyberbullying (see DfE guidance on Cyberbullying) and guidance on use of social media above.
- Raising awareness with parents/carers, as with E-safety, is crucial. The recent government guidance for parents and carers provides a useful summary and links. https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Responding to Cyberbullying checklist

Ensure that you have a consistent and comprehensive system for **monitoring and recording** cyberbullying which allows you to analyse incident records, notice any patterns and plan and review your response. Oxfordshire has a recommended system for recording behaviour and bullying incidents can be accessed here Form for recording prejudice-related incidents and bullying (doc format, 116KB)

- Try to contain the incident when content has been circulated to other people.

Report the incident to the relevant people (such as your manager, your school's Anti-Bullying Co-ordinator, and the students' parents) and to organisations (such as the internet or mobile provider, your local authority, and, in some cases, the police).

- Contact the young person's parents/carers in line with your Anti-Bullying policy
- Investigate and record all incidents of cyberbullying.
- Work with the person responsible for the bullying once they have been identified to make them aware of the consequences of their actions and try to change their behaviour - take into account anyone who passed on emails or texts or posted responses online.
- Apply disciplinary sanctions as outlined in your behaviour and Anti-Bullying policy. Consider whether a restorative approach to resolving the matter might be appropriate.
- Consider whether the matter should be reported to the police – the age of criminal responsibility is 10. See below regarding laws that may have been broken

Giving advice to young people – NB ensure you use language you know they understand to take account of age, maturity and special needs. You will also need to consider how accessible links are to individual young people.

- Advise them not to reply to the person responsible or send a nasty message back
- Advise them to preserve the evidence. If you need further advice on this please contact the police by telephoning 101.
- Advise them to remove the person responsible from your friends list (if you know them) and use built-in privacy tools to block them
- Offer support and manage the incident in the same way you would normally manage bullying. See Oxfordshire's Check list for managing a bullying incident (docx format, 179KB)
- Provide details for Childline, the NSPCC or Samaritans if they would like to speak to someone in confidence about what has happened.
- Further information on internet safety and cyberbullying for children and young people is available on Oxfordshire youth website www.oxme.info

Reporting to the police

Although cyberbullying is not a specific criminal offence in UK law, criminal laws such as the Protection from Harassment Act 1997 and the Crime and Disorder Act 1998 may apply in terms of harassment or threatening behaviour. Where mobile phone bullying is concerned, the Telecoms Act 1984 makes it a criminal offence to make anonymous or abusive calls and, if you are harassed persistently on your mobile, it may be an offence under the 1997 Harassment Act. NB. Furthermore, the Communications Act 2003 makes it a criminal offence to send: "...by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character".

In relation to sexting (the possession and sending of indecent images of children under 18) this is an offence under the Sexual Offences Act 2003 for the person sending it and the person receiving it. This could mean young people who pass on indecent images taken of boyfriend/girlfriends/picture taken of others could be committing a sexual offence and could find themselves on the Sex Offenders register. If you are concerned about how to deal with matters that may be criminal, including how and whether to view evidence that involves indecent images please contact either your police schools liaison officer or telephone the police enquiry number on 101 for further advice.

Cyberbullying information for Parents and Carers

(Adapted from www.anti-bullyingalliance.org.uk)

With increasing numbers of primary age children using social networking sites and getting their first mobile phone, it is really important that those closest to children and young people are able to help and support them. They need to learn how to stay safe and use technology responsibly early and to continue to be supported with this issue as they grow older.

Signs of bullying

You may be unsure if your child is being bullied. If you suspect this may be happening look out for the following signs. For example your child could:

- show signs of stress – being moody, silent or crying, or bullying a younger sibling or friend
- make excuses to miss school, such as stomach complaints or headaches (or your child may be skipping school altogether)
- seem upset after using the internet or mobile, or change their behaviour – for example, no longer wanting to look at new text messages immediately and be secretive and unwilling to talk about their online activities and phone use
- be withdrawn in their behaviour have more bruises or scrapes than usual
- change their eating habits
- have torn clothes, school things that are broken or missing, or have 'lost' money
- sleep badly
- be wetting the bed.

There could be other reasons for these signs, so you need to ask yourself:

- Could there be anything else bothering your child?
- Could there be changes in your family life like a new baby, or divorce or separation that may be affecting your child's behaviour?

When a child is the target of cyberbullying, they can feel alone and misunderstood. It is therefore vital that, as a parent or carer, you know how to support your child if they are caught up in cyberbullying.

Preventing cyberbullying

- Be aware of what cyberbullying is and how it can happen by looking at helpful internet sites like http://www.bbc.co.uk/schools/parents/cyber_bullying/
- Agree on family rules and procedures about what to do if someone is being cyberbullied, such as saving the message or text as evidence and telling a trusted adult.
- With your children, explore the online technologies and websites they like to use
- Become your child's 'friend' on Facebook or MSN. Have your child show you, or learn together, how to block someone on a chat service like MSN or how to report abuse to a website or service provider.
- Encourage positive use of technology by helping your child to use it to support learning, socialise with peers and explore the wider world. Discuss and promote 'netiquette' – responsible online behaviour – and reward your child for this. Tell them this means they should:

✓ respect others online – treat them how you would want to be treated

- ✓ only post or write things online and in text messages that you'd be happy for anyone to see
- ✓ use appropriate language when chatting or playing games online
- ✓ pay close attention to a website's terms and conditions and make sure you're old enough to be using a site or online service.

Support your child in making responsible decisions on the internet and when using a mobile phone – make sure they are aware of the types of photos and other content that are appropriate to post online (e.g. no photos in a school blazer or sports uniform).

Be aware that as well as being at risk, your child could also be involved in cyberbullying. Be alert to changes in your child's behaviour – especially after using the internet or their mobile phone. Discuss the emotional impact of bullying on another person.

Encourage your children to keep passwords safe. Treat your password like your toothbrush – don't share it with anyone!

Responding to cyberbullying

- Support and encourage your child if they tell you they've been cyberbullied – reassure them that it's not their fault and that they've made the right choice by reporting it to you. Tell them that bullying is not acceptable and inform them of what you will do next by following the tips below.
- Make sure your child does not retaliate or reply to cyberbullying messages of any kind.
- Help your child to save evidence of cyberbullying. Use online tools or the 'print screen' button on your computer and don't delete text messages on a mobile phone.
- If you need to, you can help your child to change their contact details (email, online username, mobile phone number) to prevent further bullying. Denying them access to the technologies is not the answer.
- Use the security tools on your family's computer, on websites or on your child's mobile phone.
- Report cyberbullying. You can report the incident to your child's school, the website or service provider, and, in serious cases, the police.

- **For further support and advice contact the following organisations.**

- **Childnet international** www.childnet-int.org A non-profit organisation working with others to "help make the Internet a great and safe place for children" which contains useful advice and information for both parent/carers and young people.
- **The Child Exploitation and Online Protection Centre (CEOP):** www.thinkuknow.co.uk .The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. CEOP also provides help and advice on cyberbullying and maintains a website for children and young people about staying safe online.
- **Parent Protect** www.parentprotect.co.uk

- **Family Lives: 0808 800 2222** Immediate support and advice for parents, 24 hours a day, seven days a week.

- **Kidscape: 08451 205 204** A telephone helpline for parents and carers of bullied children.

- **Children's Legal Centre: 08451 202948** Free legal advice on all aspects of the law affecting children and young people.

Oxfordshire

- **Oxfordshire web pages for parent/carers on bullying including cyberbullying** www.oxfordshire.gov.uk/anti-bullying **and internet safety** www.oxfordshire.gov.uk/cms/content/internet-safety-advice

- **Oxfordshire Family Information Service: Phone 08452 262636 or 01865 328580** (Mon – Thurs 9am – 5pm; Fri 9am – 4pm). Information and support for families

- **Oxfordshire Parent Partnership** Parent Partnership Oxfordshire offers impartial information, support, advice and training to parents to enable them to make informed decisions about their child's special educational needs. 01865 810516

- **Thames Valley Police** can be contacted to report a crime or seek advice on the non-emergency number **101**

National organisations who support parents/carers of children with Special Needs

- **National Deaf Children's Society: 020 7490 8656** www.ndcs.org.uk

- **National Autistic Society: 0207 833 2200** www.nas.org.uk

- **Downs Syndrome Educational Trust : 023 9285 5330** www.downsed.org www.down-syndrome.info

- **Cerebral Palsy Helpline: 0808 800 333** www.scope.org.uk

- **Contact a Family: 0808 8083555** www.cafamily.org.uk (provides support and advice to the families of children with special needs and links to various support groups

- **LOOK (National Federation of Families with Visually Impaired Children) 0121 428 5038** www.look-uk.org

- **Sense (for people with deaf blindness and associated disabilities) 020 7272 7774** www.sense.org.uk

- **Afasic (for speech, language and communication impairments) 020 7490 9410** www.afasic.org.uk www.talkingpoint.org.uk