Great Sampford Community Primary School

Online Safety Policy

September 2022

Contents

	Page
Introduction	**3**
Background	**4**
Risks	**5**
Forms of abuse through Internet Digital Mobile Technology	**6**
Why do we need an online safety policy?	**7**
Objectives	**7**
Objective 1: Ensuring that all children, young people & parents/carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world.	**8**
Objective 2: Ensure that all people who work with children and young people have access to effective policies and procedures and effective training to safeguarding children at risk through online activity.	**11**
2.1 – Filtering	**12**
2.2 – Email	**13**
2.3 – Mobile Phone	**14**
2.4 – Social Networking	**15**
2.5 - Cyber-bullying	**18**
2.6 – Publishing young people's images and work	**20**
2.7 – Illegal downloading	**21**

Objective 3: Ensure that professional know how to respond when concerns arise regarding the misuse of communications technology.	**21**
3.1 – Online safety complaints	**21**
3.2 – Monitoring online safety incidents and reporting abuse	**22**
3.3 – Staff engagement	**22**
3.4 – How do we respond?	**23**
Committing an illegal Act – Did you know?	**24**
What to do with suspicious email received at work	**25**
Appendix 1 – Glossary	**26**
Appendix 2 – Notes on the legal framework	**30**
Appendix 3 – Sources of External ICT Support	**36**
Appendix 4 – Sources of External ICT Support	**41**

Introduction

The following whole-school policy refers to the safe, acceptable and responsible use of the Internet and, mobile and on-line technologies. At Great Sampford we believe:

that all children and young people, all parents/carers and foster carers and all those working with children and young people recognise the risks, dangers and potential harm that may arise from the use of Internet Digital and Mobile Technologies. That they understand how to mitigate these risks and potential dangers and that they are able to recognise, challenge and respond appropriately to any online safety concerns so that children and young people and vulnerable adults are kept safe.

Online safety encompasses Internet technologies, electronic communications and mobile devices that use the Internet; all of which are widely used throughout the school to aid and enhance learning and promote creativity. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

As part of our commitment to learning and achievement, we at Great Sampford Primary School want to ensure that the Internet and other on-line technologies are used to:

- Raise educational standards and promote pupil achievement.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding of the world in which they live.
- Support our Independent Learner agenda.

To enable this to happen we have taken a whole school approach to Online safety which includes: the development of policies and practices, the education and training of staff, pupils and parents/carers and the effective use of the School's ICT infrastructure and technologies. We are committed to ensuring that **all** its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents/carers, are educated as to the risks that exist so that they can take an active part in safeguarding children.

The nominated persons for the implementation of the School's online safety policy are: Miss Swain, Computing Co-ordinator and Mr Athanasiou, Head Teacher.

Background

Article 17 of the United Nations Convention on Rights of the Child (UNCRC) states that, "Children have the right to get information that is important to their health and well-being. Governments should encourage mass media - radio, television, newspaper and internet content sources - to provide information that children can understand and to not promote materials that could harm children."
The Sexual Offences Act 2003[1] includes a number of offences related to child abuse online.

At Great Sampford we are aware that the understanding and use of Internet, Digital and Mobile Technology (IDMT) is essential to helping and encouraging every child to reach their full potential. As a school it is our duty to raise awareness and educate those involved in children's welfare and development about the dangers that children and young people can face in the online world, whilst accepting that safety in the online world is **not the removal or banning of access to digital technologies in itself** but rather education and training, for both children and adults, around responsible use and potential dangers.

The policy applies to:

- all pupils,
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

This policy will ensure that the school has in place:

- a range of policies (including acceptable use) that are frequently reviewed and updated;
- information made available to parents/carers that highlights safe practice for children and young people when using the internet and other digital technologies;
- adequate training opportunities for staff and volunteers;
- adequate supervision of pupils when using the internet and digital technologies;
- education that is aimed at ensuring safe use of internet and digital technologies;
- a robust reporting procedure for abuse and misuse.

[1] www.homeoffice.gov.uk/documents/adults-safe-fr-sex-harm-leaflet

Risks

Children and young people do not always recognise the inherent dangers of the internet and often do not understand that online behaviour may have offline consequences.

Despite this, digital technologies can offer them opportunities to learn and develop, communicate, be creative and be entertained. The advantages of the internet can and should out-weigh the disadvantages.

However, we now have a greater understanding to the extent of the risks the digital world can pose to children.

Risks include:

The Byron review classifies the risks inherent in the use of new technologies as relating to content, contact and conduct. The risk is often determined by behaviours rather than the technologies themselves:

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/ advice

Byron review of Children and new technology (2008) Published by DCSF and DCMS

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information

- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
- Exposure to illegal material, such as images of child abuse.

Contact

- Grooming using communication technologies to meet and groom children with the intention of sexually abusing them (both on and off line exploitation).

Commerce/Conduct

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

BECTA (2007) identify some of the issues which are summarised below.

Forms of Abuse through Internet Digital and Mobile Technologies (IDMT)

- Children and young people have been 'groomed' online by adults (often pretending to be those who care) with the ultimate aim of exploiting them sexually.
- Children / young people have been bullied by other young people via social networking sites, websites, instant messaging and text messages; this is often known as 'cyber-bullying'.
- Inappropriate (i.e. threatening, indecent or pornographic) images of children and young people have been taken, uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube, often by other young people. This is a criminal offence under s45 of the Sexual Offences Act 2003.
- The dangers attached to gang culture can rapidly accelerate online as many gangs 'advertise' or promote themselves via websites or social networking sites or if threats of violence, threats to an individual's life or threats of retaliation are posted online by opposing gang members.
- Unsuitable websites and images can easily be accessed online.
- Images of physical abuse, crime, racism, self-harm, terrorism or on physical violence to influence young minds.

At Great Sampford we understand that ignoring the dangers that children/young people/parents/carers can face would lead to serious gaps in our responsibilities towards safeguarding and child protection.

Why do we need an online safety policy?

Each new technology introduces new opportunities and challenges for children and young people, parents/carers and those working with young people. In order to minimise the risks involved from new technologies we need to understand how children and young people use IDMT and how this may be misused by those who may present a risk to children. It is important that we know how to respond when concerns arise.

In recent years the internet and other means of electronic communications have become increasingly accessible to children and young people. This provides great opportunities for young people in terms of education, information, communication and having fun. However, it also includes risks from those intent on sexually exploiting children and from the inappropriate use of communications technology. This highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It also highlights the need to provide appropriate guidance to those working with children and parents/carers.

Objectives

All organisations that work with children and young people need to have an e-policy in place based on the following three objectives:

1. ***Ensuring*** *that all children, young people, parents/carers and foster carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world;*

2. ***Ensuring*** *that all people who work with children & young people have access to effective policies and procedures and effective training to safeguard children at risk through online activity; and*

3. ***Ensuring*** *that professionals know how to respond when concerns arise regarding the misuse of communications technology.*

Objective 1: *Ensuring that all children, young people, parents/carers and foster carers should be equipped with the knowledge and skills to safeguard themselves in the online/digital world;*

Great Sampford Primary School recognises that the Internet and other digital technologies can: transform learning, help to improve outcomes for children and young people, and promote creativity; all of which add up to a more exciting and challenging learning experience.

As part of achieving this we want to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to develop the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

To this end, Great Sampford Primary School will:-

- Enable all pupils to develop and exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum.
- Train all school staff so that they are equipped to support pupils in gaining positive experiences when online and also help pupils develop strategies if they encounter a problem.
- Support parents/carers in: gaining an appreciation of how to stay safe on-line, internet safety for both themselves and their children, providing them with relevant information on the policies and procedures that govern the use of Internet and other digital technologies within the school.

To facilitate this, Online safety education will be provided in the following ways:

Online safety within the Curriculum

Early Years Foundation Stage and Key Stage 1
At this level, use of the Internet will either be heavily supervised or based around pre-selected, safe websites and apps. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about.

Lower Key Stage 2
Children will be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children,). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be overtly taught.

Upper Key Stage 2
Children will be encouraged to become more independent at researching for information on the World Wide Web, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach the children how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

Training for Staff and Governors

Staff and governors receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues.

Training for Parents/Carers

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies; just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive online safety education and information (e.g. via the school website and twilight training provided as required) to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good online safety behaviour.

Listed below are useful websites that parents, staff and governors are made aware of (if appropriate) to further their knowledge and understanding of online safety and its implications for young people:

www.thinkuknow.co.uk and www.ceop.co.uk
The Child Exploitation and Online protection (CEOP) centre delivers a multi-agency service dedicated to tackling and bringing offenders to account either directly or with local and international police forces and working with children and parents to deliver their ThinkuKnow internet safety programme. Much of the online safety taught in Great Sampford Primary School is based on this material.

http://www.iwf.org.uk/
The Internet Watch Foundation was established in 1996 by UK internet industry to provide an internet hotline for public and IT professionals to report potentially illegal online content with the intention of having the offending material removed.

www.pitda.co.uk
Parenting in the digital age

http://www.childnet.com/resources/esafety-and-computing
Childnet are an international organisation focussed on providing essential materials for teachers, parents and carers. This web resource offers a lot of resources used for the delivery of the Key Stage 2 online safety curriculum.

Objective 2: *Ensuring that all people who work with children & young people have access to effective policies and procedures and effective training to safeguard children at risk through online activity*

The Internet Digital and Mobile Technologies are constantly developing and evolving and this section is only intended to give an idea of the range of communications channels used by people to contact each other and exchange electronic data - including Child abuse images.

All users must be compliant to our Acceptable Use Policy (AUP) for example:

- not act un-reasonably and be inconsiderate of other service users.
- must take responsibility for their own network use
- Computer and internet access should have appropriate security and anti-virus protection.
- Must ensure to not disable or circumvent security measures – filters, encryption etc.
- Must not have personal and sensitive electronic data taken offsite without being security encrypted and authorised by management.
- Must not have unapproved software being introduced into local networks and not authorised by management.

Users shall not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children,
- Promoting discrimination of any kind,
- Promoting racial or religious hatred,
- Promoting illegal acts
- Any other information which may be offensive to peers or colleagues e.g. abusive images; promotion of violence; gambling; criminally racist or religious hatred material.

2.1 Filtering

The Internet Digital and Mobile Technologies are constantly developing and evolving and this section is only intended to give an idea of the range of communications channels used by people to contact each other and exchange electronic data - including Child abuse images. All access to the Internet at Great Sampford Primary School is filtered through our provider. This filtering system provides the following:

- Subscribes to the Internet Watch Foundation (IWF) filtering list. This will help to filter out some inappropriate content, but not all.

- Levels of internet access and supervision IS age appropriate and suitable for the young people and is secure but adaptable.
- Staff have access to a normally restricted websites for children in order to carry out research for planning and/or produce and obtain resources. This access is never available to the children.

- Access controls (filtering) prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day and this is vigilantly upheld by our internet provider.

- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
- Management should ensure that regular checks are made to ensure that filtering methods selected are age appropriate, effective and reasonable. Access to inappropriate websites any material perceived to be illegal must be reported to management who should inform this to the appropriate agency.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative),
- Adult material that potentially breaches the Obscene Publications Act in the UK,
- Criminally racist or anti-religious material,
- Violence and bomb making,
- Illegal taking or promotion of drugs,
- Software piracy,
- Other criminal activity

2.2 Email

- Email is now an essential means of communication which can also be accessed via most mobile phones. A degree of responsibility has to sit with children, young people and professionals since as soon as email access is permitted it is very difficult to control. Restricting both incoming and outgoing email to specific addresses is possible, however, not always practical as addresses can easily be changed. Microsoft Office 365 mail used by all staff at Great Sampford is scanned and filtered for spam and has an editable abusive language filter. Staff and Governors must only use school email addresses for school business.
- Email should not automatically be considered private and most organisations reserve the right to monitor email. However, there has to be a balance between maintaining the safety of children/young people and their rights to privacy, which are covered by legislation.
- Email content and tone must also be considered. Due to the impersonal nature of email, children and young people may write things or be aggressive or dismissive in tone which may be hurtful to others, even if such content or tone is not intended it may still be considered as cyber-bullying. In upper Key Stage 2 all children are taught the impact of and how to be safe using email. All e-mail accounts provided to the children are kept anonymous to protect their identity. These emails are also tracked and stored even if deleted on a users device (such as a phone or tablet). This is to ensure we can closely monitor e-mails if required or ensure that crucial evidence is not lost. This is further explained under section 2.3 Mobile Devices.

- Young people are encouraged to be creative and non-identifiable in setting up personal email addresses.

All users of the Internet and email at Great Sampford must understand that they may not:

Reveal or publicise confidential or proprietary information, which includes - but is not limited to:

- Financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.

Undertake activities with any of the following characteristics:

- corrupting or destroying other users' data;
- violating the privacy of other users;
- disrupting the work of other users;
- deliberate introduction of viruses;
- use any mobile or digital technologies providing access to any internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

2.3 Mobile Devices

Most young people now have access to mobile telephones which are generally perceived as essential to their day to day living and communicating and now offer access to the internet, instant messaging, email, social networking, a camera and video facilities. At Great Sampford Primary School we now facilitate the opportunity for each child to use an iPad and laptop. We believe that whilst not only enhancing the children's learning, it gives us (the school) the perfect platform in which to educate children and make them aware of the risks associated with mobile devices in a safe environment. We believe that this will provide the children with the appropriate skills to keep them selves safe as they progress up into their teenage years.

Through this provision the children understand:

- We only share telephone numbers and other contact details with those known to them and ensure that electronic records (call, text and email logs) are kept of any bullying or threatening telephone calls, text messages, emails or images received which may need to be used as evidence in resolving issues or to be provided in any police investigation.
- We should be careful about accepting invitations to join location based social networking sites and that the required age for most of these is 13 years old.
- Content sent and received via a mobile device is tracked and monitored by third parties. We (the school) have access to and monitor all school email addresses and have access to content even when it has been deleted from a device.
- School restricts the use of mobile devices during working hours.

At Great Sampford Primary School we restrict the use of staff mobile devices during work 'contact' hours in order to protect our children. This is to protect both pupils and staff.

2.4 Social Networking

The Internet provides ready access to online spaces and social networking sites which allow individuals to publish un-moderated content. Social networking sites such as Facebook, Twitter, Chat Rooms, Online Gaming Platforms and Instant Messaging can connect individuals to groups of people which may be friends in the 'virtual' world but who may have never met each other in the real world. Users can be invited to join groups and leave comments over which there may be limited or no control.

At Great Sampford Primary School:

Children are encouraged to consider the associated risks and dangers related to sending or accepting friend requests and posting personal comments, inappropriate images or videos about themselves or their peers and the subsequent difficulty in removing an inappropriate image or information once published. They should also be advised not to publish detailed private thoughts or emotions which could be considered threatening, intimidating or hurtful to others.

Children are taught to understand why we should never give out any personal details or images which may identify themselves, their peers, their siblings / foster siblings, their location or any groups, schools or organisations they attend or associate with. This includes real names, dates of birth, address, phone numbers, e-mail addresses, photographs or videos, school attended, IM and email addresses, including those of friends, family / foster family and peers. This also includes any 'gangs' they may be affiliated with.

Children are advised about e-security and encouraged to communicate with known friends and family only and deny access to others by making their profiles private.

Care is taken to delete old and unused profiles from websites which are no longer used as these will remain accessible to others. Personal information voluntarily shared by a young person is unlikely to remain the same as the person matures and has a greater understanding of how personal information about them can impact on their later lives (i.e. perspective employers making an online search of their name and sighting inappropriate photographs, videos or content etc.).

Teachers, governors and other staff are encouraged to familiarise themselves about the risks and inappropriateness of sharing personal information about themselves via social networking sites with young people. They should be made aware that any inappropriate material posted could affect their professional status. They must also responsibly restrict access to their friends and family only and 'friend requests' by a young person may be within professional boundaries.

Staff are also encouraged to steer clear of social networking sites that young people are known to frequent and to follow the guidance found in **Appendix 4 - Guidance on the use of Social Networking and messaging systems for staff.**

Use of Social Networking Sites in Work Time
Use of social networking applications in work time for personal use only is not permitted.

Social Networking as part of School Service
All proposals for using social networking applications as part of a school service (such as using the blog on the school website), whether they are hosted by the school or by a third party, must be approved by the Head Teacher first.

Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head Teacher. However, school representatives must still operate in line with the requirements set out within the policy.

School representatives must adhere to the following Terms of Use:
The Terms of Use below apply to all uses of social networking applications by all school representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on the school network or not.

Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Great Sampford Primary School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Terms of Use:

Social Networking applications:
- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.
- Must not be used in an abusive or hateful manner.
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with.
- Employees should not identify themselves as a representative of the school.

- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher.
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/Protection for Staff on using Social Networking

- No member of staff should interact with any pupil in the school on social networking sites unless being used as a model for safe use during the teaching of online safety in the curriculum.
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18.
- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform the Head Teacher. However, it would not be appropriate to network during the working day on school equipment.
- It is illegal for an adult to network, giving their age and status as a child.
- If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Child Protection officer in school or Head Teacher.

Child Protection Guidance

If the Head Teacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above they should:

- Record the disclosure in line with their Child Protection Policy.
- Schools must refer the matter to the LADO (Local Authority Designated Officer) who will investigate via Essex Police Child Protection Team.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes.
- If disclosure comes from a member of staff, try to maintain confidentiality.
- The LADO will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.
- If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out.

2.5 Cyber-bullying

Cyber-bullying can be defined as "*The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone*" (DCSF 2007).

We encourage children, staff and parents/carers to understand that they should find using IDMT as a positive and creative part of their everyday life. Unfortunately, IDMT can also be used negatively to target a specific young person or group or even a member of staff. At Great Sampford we take stringent steps in order to prevent this and resolve any issues that may arise.

Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school. Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted anti-bullying policy. If a parent/carer refuse to engage and bullying continues, it can be referred to the police as harassment.

Guidance on how to respond to cyber-bullying:

- A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.
- A child is receiving taunts from peers. It is all at weekends using Skype and Facebook. The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.
- A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y5: The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school, the school could legitimately say that the victims and perpetrators had failed to follow the school's recommendation. They could then deal with residual bullying in the school, but refuse to deal with the social networking issues.

This guidance applies to any form of electronic communication including text and mobile phone cyber-bullying.

We also understand that:

- Teachers and other education staff are particularly vulnerable to 'cyber-bullying' by pupils or even ex-pupils, which may include general insults, threats, harassment, defamation, homophobic or racist remarks or other forms of prejudice based bullying. The effects of cyber bullying by young people on adults are equally distressing and the impact on the victim can be just as profound – Government guidance notes remind us that cyber bullying incidents are upsetting whoever the victim is and whatever age they are.

- We should be alert to the possibility and potential for cyber bullying towards members of staff by young people and appreciate there is no single solution to the problem.
- Instances of cyber-bullying must be responded to sensitively and in line with existing anti-bullying policies and procedures in the organisation.
- The victim of cyber-bullying must be reassured they have done the right thing in disclosing the bullying and be supported. Please refer to the attached **Appendix** for further information on this. This should also be cross referenced with the local anti-bullying policy.

2.6 Publishing young people's images and work

At Great Sampford Primary School we believe in sharing and promoting our children's successes and one way we achieve this is through or school website. However, we are aware of the associated risks associated with including images or videos of children to help promote our school and follow these guidelines:

- Children are advised when photographs or video footage of them is being taken and images should never be published without the consent of the young person, and the written consent of their parent/carer or foster carer. For more information and detail on further guidance we follow can be found in our Data Protection Policy.
- Although it is fairly simple to upload comments, images and videos on social networking and video broadcasting websites, children are explicitly taught about the associated consequential risks and dangers in doing this and the difficulties in removing this content, particularly if the content subsequently becomes the property of the publisher.
- Inappropriate, offensive or threatening content can have devastating consequences to individuals and groups (including gangs) and children are made aware of the legalities and long term implications of doing this.

2.9 Illegal Downloading

Whilst there are many sites where music, videos and software can be legally downloaded, children young people and adults need to be made aware that they could be breaking the law by downloading copyright protected files or by infringing other intellectual property rights.

The various industries affected by illegal downloading (particularly music) do monitor the internet and can take legal action ranging from fines to suing those who hold parental responsibility. It is recommended that websites are thoroughly researched prior to downloading content for personal use.

Objective 3: *Ensure that Professionals know how to respond when concerns arise regarding the misuse of communications technology.*

3.1 e-safety complaints

- Any complaints about online safety concerns should be progressed via the organisations recognised complaints procedure which should be readily accessible to all; however efforts should be made to resolve low level issues internally. These must be recorded locally. See the flow chart.
- All factors in relation to the complaint must be clearly established in order to have substance.
- Complaints about employee's IDMT misuse should be escalated to the most senior manager within the organisation and be managed according to recognised disciplinary and child protection procedures.
- Employers must have internal methods of scrutinising IDMT use, in particular, the ability to identify sites accessed. This is particularly important where there is an allegation that illegal or inappropriate websites have been accessed.
- Potentially illegal issues must always be referred to the police in the first instance.

3.2 Monitoring e safety incidents and reporting abuse

Any form of electronic or digital abuse towards young people should in the first instance be reported to the Child Exploitation Online Protection service www.ceop.police.uk, and also reported to the relevant IDMT lead with the organisation. Any incidents which place a young person in immediate danger should be referred to the local police by calling 999. For further guidance on our recording and record keeping procedures, please refer to our Child Protection and Child Protection Procedure policies.

3.3 Staff Engagement

- All staff with responsibility for young people's learning via IDMT are familiarised with this policy and given opportunities to raise issues and concerns they face in their day to day working responsibilities.
- All staff must understand that misuse of IDMT will result in disciplinary action being taken against them in line with your organisations policies and procedures. Employees unsure of what constitutes acceptable usage of the internet should always check with management. They should be aware that all internet usage is monitored and can be traced back to each individual user.
- Staff are made aware of what is acceptable in terms of their engagement with children and young people via IDMT means.
- Staff (including volunteers) should never disclose or share their personal details except in certain exceptional roles (i.e. personal mobile phone numbers, email addresses or social networking profiles etc.) or send or accept friend requests on social networking websites with children and young people / service users.

- Any necessary contact between a young person and a professional should be made via equipment and contact details provided by the employer (not personal equipment / contact details) and be clearly recorded on a need to communicate basis and with the consent of the parent/carer or foster carer. Alternatively, personal contact details for children / young people should be stored centrally by management and only accessed on a need to know basis as approved by management.
- At Great Sampford Primary school we adopt an open culture of vigilance in the workplace and staff must feel confident in identifying and challenging poor and/or risky working practices. For further guidance on Safer Working Practice with Technology, please refer to the supplementary guidance in **Appendix 3.** Training on acceptable usage and responsible online safety is provided during the induction period for all new employees with a specific emphasis on professional boundaries, confidentiality and data protection. This is also continually updated and provided to all staff and parents on a two-year cycle.

3.4 How do we respond?

This section is designed to help staff determine what action they can take when they identify concerns and should be read in conjunction with our Anti-Bullying, Whistleblowing and Safeguarding policies. The response required will depend on the nature of the incident. Concerns may relate to:

- The accidental access to inappropriate material
- Accidental access to illegal material
- Deliberate access to inappropriate material
- Inappropriate or illegal use of technologies
- Bullying or harassment using technology

Committing an Illegal Act - Did You Know?

1

Receiving unsolicited emails that may contain potentially illegal material (either as an attachment or in a URL) is not an illegal offence

2

If you receive potentially illegal material you could easily commit an illegal act - **do not open the material or personally investigate**

3

Opening an attachment or URL that proves to hold illegal content **is an illegal act** and is classed as possession of illegal material

4

Showing anyone else illegal material that you have received **is an illegal act**

5

Printing a copy of the offensive email to report it to someone else **is an illegal act** and is classed as producing illegal material

6

Having printed a copy of the material if you give it to someone else **is an illegal act** and is classed as distributing illegal material

7

Within 4 simple steps you could easily break the law 4 times. Each is a serious offence

Never open unsolicited URLs or attachments. If you are suspicious that the content could be illegal report it and log that you have received it

9

Always report potential illegal content to the Internet Watch Foundation at www.iwf.org.uk They are licensed to investigate **you are not.**

Never personally investigate. If you open illegal content accidentally report it to your manager and IWF. Go to the IWF website and click on the report button. **Do not copy and paste the URL, write it down and type it into the reporting screen. This prevents accidental opening**. Once the email has been logged and reported to the IWF delete it from your inbox. If you are unsure, contact the IWF for advice on 01223 237 700. **The Internet Watch Foundation only deals with illegal content, please see their website for information and advice. Please note this guidance only relates to illegal content not inappropriate.**

What to do with suspicious email received at work

You receive an email that has potentially illegal material e.g. Child abuse images, Incitement to violence or Race hate	You receive an email that contains inappropriate content e.g. abusive or bullying content, adult sexual material etc. This email is from someone you know within your work setting	You receive an email that contains inappropriate content e.g. Adult sexual material, bad language etc. and this email is not from someone you know but is from what seems to be a 'real' (i.e. not a spam) email address	You receive an email that contains inappropriate content e.g. Adult sexual material This email is not from someone you know and appears to be a SPAM email.
Report this email to your designated child protection lead and/or manager A written log should be kept of the email and the fact that it was passed onto the IWF	Report this email to your designated person and/or Online safety officer. A written log should be kept of the email. In consultation with the Police/LADDO/appropriate person an investigation should be undertaken.	Report this email to your designated person and/ manager. A written log should be kept of the email and where it was sent for investigation	Report this email to your designated person and/or manager. A written log should be kept of the email and where it was sent for investigation
Report this email to the IWF Go to www.iwf.org.uk Click on the report button and follow the instructions and their advice.	Consider whether Module 12 of the SET Procedures applies – If yes refer to the Local authority Designated Officer	If the senders ISP is known – can a complaint be raised under their acceptable use policy if appropriate?	Report this to Easynet on abuse@uk.easynet.net

In all cases secure the email in a folder and only delete when the investigation has been completed or you are advised to do so.

In the case of potential illegal material do not show the content of this email to anyone but report it to your manager and take the advice of the Internet Watch Foundation.

Do NOT always presume that the sender's email address is telling you the truth – Spammers can and do fake other's email addresses.

If you are unsure how to proceed please contact the Northern Grid for Learning on 0191 4611844

Appendix 1 - Glossary

Acceptable use: A policy that a user must agree to abide by policy (AUP) in order to gain access to a network or the internet. It may also cover how other communications devices, such as mobile phones and camera phones, can be used on the premises.

Adware: A program that appears to be free but may be paid for by companies whose products are advertised every time you use it. Some adware contains small programs that track the websites you visit on the internet, reporting the information back to marketing sites which then tailor advertisements to your interests. This is similar to spyware. The most sophisticated spyware can even track what keys you are hitting when you type, so using a **firewall** is vital to filter out these kinds of programs.

Avatar: A graphical representation of a person. Avatars are sometimes used in chat and multi-user gaming environments.

Blog: A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors.

Bluetooth: Bluetooth is a telecommunications industry standard which allows mobile phones, computers and PDAs to connect using a short-range wireless connection.

Bookmarking: The process of storing the address of a website or internet document on your computer, so that you can find it again easily.

Chatroom: An area on the internet or other computer network where users can communicate in real time, often about a specific topic. As chat software develops, individuals are not only able to send text messages to chat rooms but, in some instances, also have the ability to communicate through their actual voices (voice chat) via headsets, or indeed, actually be seen by chat room members, through web cams.

When joining a chat service or room an individual must select an onscreen name or nickname, and all members of a chat room are usually listed down one side of the screen. As well as chatting in a specific room, individuals can request and initiate private conversations with other members of a chat room, which can appear similar to instant messaging.

Cookie: a piece of data stored in your computer after you have visited a website, that allows the web page to be down loaded more quickly.

Cyberspace: *Cyberspace* is a metaphor for the environment in which communication over computer networks occurs. The word is often used as an alternative to *internet*.

Digital video: Video captured, manipulated and stored in a digital format.

Filtering: A method used to prevent or block users' access to unsuitable material on the internet.

Firewall: A network security system used to restrict external and internal traffic.

Hacking: The process of illegally breaking into someone else's computer system breaching the computer's security.

Internet service provider (ISP): A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

Instant messaging (IM): Allows users to communicate with other users, providing an easy way of sending short written messages to a few friends online at the same time. It includes text messaging, voice chat, webcams, and file and picture exchange. IM can be a very private form of communication between known friends where the user builds up a list of contacts and is alerted when they are online. IM, however, can also be a public open environment where the user is encouraged to find and make new contacts online.

P2P (peer to peer): The internet is beginning to offer new services alongside websites and chat services, particularly those which enable the swapping and storing of media files (sounds, images and video). This is referred to as *Web 2.0*. These services can enable direct sharing of files – person to person, computer to computer. These services are much harder to moderate than chat rooms and message boards. As ISPs and service operators bring in moderation to make sure their digital services with a social function are safer for children, technology is encouraging social activity away from these safe centres. This means that educating children and young people how to protect themselves online becomes even more important.

Personal digital assistant (PDA): A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.

Phishing: When someone tricks you into giving confidential information by asking you to click on a false website and entering your details.
Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

SMS: Short messaging service or text messages.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan horses: A virus which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user.

Usenet: The part of the internet where **newsgroups** are found.

Video conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Vlog: A **blog** which showcases video.

Virus: A computer program which enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

WAP: A website designed to be accessed on a small screen like a mobile phone.

Webcam: A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.

Weblog: See the entry for 'blog' above.

WIFI: Short for wireless fidelity, it is a way of connecting a computer to the internet using radio frequency, rather than cables. A hotspot is where you can access a WIFI network.

Appendix 2 - Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of communications. Many people use the Internet regularly without being aware that some of the activities they take part in are potentially illegal.

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, Connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

"Organisations have a right (and in the case of providing services to children, a duty) to monitor use of their technical infrastructures to prevent them being used inappropriately, for unlawful purposes or to distribute offensive material.

However, an individual also has a right to privacy. It is the duty of any organisation that provides online access to balance these two separate rights and, in the case of children's and community services, different policies may be needed for children and adults within these settings.

In any case, organisations should be open on the subject of monitoring the use of their technical networks, and this can typically be achieved through the acceptable use policy, as previously discussed." (BECTA)

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.

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

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

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

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

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

Regulation of Investigatory Powers Act 2000

"The Regulation of Investigatory Powers Act (RIPA) provides the legal framework for using methods of surveillance and information gathering to help the prevention of crime. It includes, among other provisions, the interception of communications, the acquisition and disclosure of data relating to communications, and access to electronic data protected by encryption or passwords.

Each police force and most councils are defined as a 'public authority' to which RIPA applies. The forms of surveillance that the police and any council are entitled to authorise are covert directed surveillance and the use of covert human intelligence sources (informants). In any council, only officers of the rank of deputy chief officer and above may be designated as authorising officers under RIPA. No covert directed surveillance or use of covert human intelligence sources may be undertaken without obtaining authority from such an authorising officer.

RIPA requires that third parties that are required to provide information about other people subject to surveillance and investigation should be approached for that information in a highly controlled manner by means of standard forms published by the Home Office.

It is possible that, in their role of safeguarding children, LSCBs and member agencies may be subject to the provisions of RIPA. As such, they should be aware of the appropriate response if such a request is made." (Ref: BECTA 2007)

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.
Internet use and abuse is governed by many civil or criminal laws in the UK. While this list is not exhaustive, some of the key provisions are summarised below:

- Computer Misuse Act 1990 (including hacking, denial of service attacks)
  http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

- Copyright, Designs and Patents Act 1988(including copyright theft)
  http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

- Crime and Disorder Act 1998
  http://www.opsi.gov.uk/acts/acts1998/19980037.htm

- Data Protection Act 1998
  http://www.opsi.gov.uk/acts/acts1998/19980029.htm

- Privacy and Electronic Communications (EC Directive) Regulations 2003(including spam)
  http://www.opsi.gov.uk/si/si2003/20032426.htm

- Protection from Harassment Act 1997 (including harassment, bullying, and cyber stalking)
  http://www.opsi.gov.uk/acts/acts1997/1997040.htm

- Protection of Children Act 1978, as amended by Section 84 of the Criminal Justice and Public Order Act 1994 (including indecent images of children)
  http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

- Malicious Communications Act 1988 (including harassment, bullying, and cyber stalking)
  http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

- Sexual Offences Act 2003 (including grooming)
  http://www.opsi.gov.uk/acts/acts2003/20030042.htm

- The Obscene Publications Act 1959 and 1964 (including illegal material on, or transmitted via, the web and electronic communications) - not available online

- The Telecommunications Act 1984 (including illegal material on, or transmitted via, the web and electronic communications) - Not available online

Appendix 3 - Sources of external online safety support

There are a number of agencies that can provide help either in terms of providing training on online safety issues, responding to specific online safety incidents, or supporting the key stakeholders in a child life. Some of these are described briefly below.

Child Exploitation and Online Protection Centre
[http://www.ceop.gov.uk]

The Child Exploitation and Online Protection (CEOP) Centre aims to tackle child sex abuse wherever and whenever it happens. Part of their strategy for achieving this is to provide internet safety advice for parents and carers, training for educators and child protection professionals, and providing a 'virtual police station' for reporting abuse on the internet.

Some of these services are outlined briefly below.

Thinkuknow – online safety for young people and their parents
[http://www.thinkuknow.co.uk]

The CEOP Thinkuknow website provides a range of information on online safety for young people, with key topics including mobiles, gaming, social networking, chatting, podcasts, blogs, and peer-to-peer TV.
The content of the site is based around three key messages:

- How to have fun online
- How to stay in control online
- How to report online.

A section of the website is aimed specifically at parents and carers to try to help them understand more about what their child may be doing online.
The site also provides a prominent link to the CEOP report abuse service for reporting suspicious behaviour online with or towards a child (see below).

Training for educators
[http://www.thinkuknow.co.uk/teachers]
CEOP offers training to educational professionals through the Thinkuknow Education Programme, aimed at children aged 11-16.

Once trained, educators are able to directly deliver the Thinkuknow programme to children. Further completion of the CEOP Ambassador Training scheme will also allow educators to cascade the training to colleagues. The authority has a trained CEOP Ambassador so if your schools would like some training, please contact Mark Churchill.

Training for child protection professionals
http://www.ceop.gov.uk/training/courses.html

CEOP work alongside colleagues in the criminal justice and child protection agencies in the UK and abroad to add value to existing services and provide greater support to professionals working in this area.

They provide a series of specialist training courses aimed at professionals who:

- conduct criminal investigations where the sexual abuse of children is a factor
- manage offenders in the community or within the justice system
- take responsibility for safeguarding children from sexual predators.

The training courses are designed to help delegates better understand the nature of sexual offending and to develop the skills and knowledge that can better equip professionals to deal with the very difficult and distressing nature of such crimes. One of the courses deals specifically with internet sex offenders.

Reporting abuse

CEOP provides a facility, in association with the Virtual Global Taskforce, to report any inappropriate or potentially illegal activity towards a child online. This might be an online conversation with someone who a child thinks may be an adult, who is treating a child in a way which makes them feel uncomfortable, or who is trying to meet a child for sex.

If a child is in immediate danger, dial 999 for immediate police assistance.

There are prominent reporting links from the CEOP website, the Virtual Global Taskforce website and the Thinkuknow website. A reporting link is also available as a tab option in MSN Messenger.

Virtual Global Taskforce
http://www.virtualglobaltaskforce.com

The Virtual Global Taskforce (VGT) is made up of law enforcement agencies from around the world working together to fight child abuse online. The aim of the VGT is to build an effective, international partnership of law enforcement agencies that helps to protect children from online child abuse.

A section for young people provides links to a range of useful resources, and the site also provides a direct link for reporting abuse.

Internet Watch Foundation
http://www.iwf.org.uk

The Internet Watch Foundation (IWF) is the UK hotline for reporting illegal content, specifically child abuse images hosted worldwide and content that is criminally obscene and incitement to racial hatred, hosted in the UK. A prominent link for reporting illegal content is available from the homepage of the IWF website.

The IWF website also provides an overview of the IWF URL list of online child abuse content, which should be included as an absolute minimum in internet filtering services

NSPCC and related services
http://www.nspcc.org.uk

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

NSPCC services include ChildLine, a free and confidential helpline for children in danger and distress. Children and young people in the UK can call 0800 1111 to talk about any problem, 24 hours a day.

There4me.com

There4me.com is an online advice and information service specifically aimed at children aged 12 – 16, covering topics such as internet safety, abuse and bullying. Services include message boards, a private online in-box, and 'real time' one-to-one counselling with NSPCC advisers.

Child Protection Helpline

The NSPCC Child Protection Helpline offers advice and support to anyone concerned about the welfare of a child. The helpline is a free, confidential service open 24 hours a day, seven days a week on 0808 800 5000

Stop it Now!
http://www.stopitnow.org.uk

Stop it Now! aims to prevent child sexual abuse by increasing public awareness and empowering people to act responsibly to protect children.

Stop it Now! operates a freephone helpline on 0808 1000 900. It offers confidential advice and support to adults that might be unsure or worried about their own thoughts or behaviour towards children, or the behaviour of someone they know, whether they are an adult or a child.

Experienced advisors are available to discuss concerns and can offer confidential advice and guidance on an appropriate course of action.

(Adapted from BECTA: safeguarding children in a digital world: Developing an LSCB online safety strategy)

Bullying online
http://www.bullying.co.uk

Bullying Online is an online help and advice service combating all forms of bullying. Recognising that many young people that have lost friends through being bullied in the real world may turn to the internet to make new friends, the 'Staying safe in cyberspace' section gives tips for staying safe in chat rooms. There is also a section on mobile phone bullying, giving tips on how to protect yourself, and information on how the law can help. The site provides information for pupils, teachers and parents.

Parentscentre
http://www.parentscentre.gov.uk

Parentscentre offers support, information and advice on children's learning and the education system, including use of the internet.

Safer working practices for adults working with technology with children and young people

Professionals (including volunteers) working with children and young people must appreciate the nature and responsibilities of their professional roles that places them in a position of trust with children and young people.
Guidance to safer working practices with technology aims to:
Ensure that children and young people are safeguarded in the digital world

Provide professionals with advice and good practice, and work towards a culture of vigilance in workplace.
Assist professionals to comply with their own Codes of Practices/ Acceptable Use of Internet policies
Minimise risks of allegations of abuse or inappropriate behaviours against staff members.
Project a clear message that unlawful or unsafe / risky behaviours with IDMT are unacceptable and disciplinary action will be taken in line with council policies.

Appendix 4 - Guidance on the use of Social Networking and messaging systems for staff

The school recognises that many staff will actively use *Facebook*, *Twitter* and other such: social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks – discretion and professional conduct is essential. They are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

In accordance with school's Safeguarding and *Child Protection Policy*, it is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors to again avoid any possible misinterpretation of their motives or behaviour which could be construed as grooming.

Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. All correspondence should be via school systems.

It is also important for staff to note that Facebook is targeted at older teenagers and adults. They have a no under 13 registration policy and recommend parental guidance for 13 to 16 year olds.

The following are extracts from Facebook privacy policy:

"*If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us*"

"*We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices.*

Materials to help parents talk to their children about safe internet use can be found on this help page."

It has also been reported that many children aged between eight and twelve have been evading the age restrictions that have been put in place on Facebook, Bebo and MySpace. As a safe school, we recognise the need to educate the children in our care to evaluate their own use of social media and how to be safe users of the Internet and mobile devices.

Acknowledgments

This document draws upon existing good practice and guidance provided by:

BECTA (2007) Safeguarding children online: a check list for Local Authorities and Local Safeguarding Children Boards
BECTA (2008) Safeguarding Children in a digital world
Internet Abuse Guidelines 2010, Essex and London Safeguarding Children Boards
CEOP www.ceop.org.uk
Kent: online safety policy www.clusterweb.org.uk
North Yorkshire online safety policy
Lambeth online safety policy