LYDIARD MILLICENT CE VC PRIMARY SCHOOL

E-SAFETY POLICY

Member of staff responsible	Paula Kilkelly
Governor responsible	Governor Responsible
Committee responsible	Performance
Date agreed with staff	11th March 2016
Date discussed with pupils	10th March 2016
Date agreed at Committee	20th April 2016
Date approved at Governing Body	11th May 2016
Frequency of policy review	Triennial
Date next review due	Feb 2019

Document Version Control

Issue Number	Issue Date	Summary of changes
1.0	Feb 09	New Policy
1.1		County amendments
1.2	Feb 10	Reflects pupils views
1.3	Feb 13	Cyber-bullying added (section 11.4) Mobile Technology section updated (section 11.3)
1.4	Feb 16	References to ICT changed to Computing changed, where relevant, in line with New Curriculum. References to Wiltshire CC and SWGFL changed to Technical Support Team (Oakford Technology). Committee name updated. Radicalisation added. (section 3.2) Prevent Duty link added (section 16.1) Responsible Internet Use rules updated. (P13) Policy for responsible e-mail, network and Internet use for Lydiard Millicent School (P 15) Lydiard Millicent Primary School - Guardian Letter (P16) Laptop policy for Lydiard Millicent school staff (P18) Useful Contact Details (P19) Section 7 and 8: Internet Access and Filtering (Page 6 and 7) Section 10: Managing content (page 7 and 8) Laptop, computer and Internet policy use for LM staff

CONTENTS Page

1. Introduction

The Internet is regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using computers. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and other mobile devices. Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

Young people have access to the Internet from many places; home, school, friends' homes, libraries, mobile phones and devices. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

2. Core Principles of Internet Safety

The Internet is as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing of pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use and the safety of pupils.

3. The e-Safety Policy is built on the following five core principles:

3.1. Guided educational use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

3.2. Risk assessment

21st century life presents dangers including violence, racism, exploitation and radicalisation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become "Internet Wise". Schools need to ensure that they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material.

Pupils may obtain Internet access in youth clubs, libraries, and public access points and in homes. Ideally a similar approach to risk assessment and Internet safety would be taken in all these locations, although risks do vary with the situation.

3.3. Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully. There are a number of technical solutions to help limit Internet access, though; it is the appropriateness and consistency of the school's e-safety policy that is of overriding importance.

3.4. Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within schools must simply be denied, for instance unmoderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

3.5. Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. ***There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.***

4. Who will write and review the policy?

Our e-safety has been written by the school and alongside government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed triennially.

5. Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

6. How will Internet use enhance learning?

The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.

Pupils will learn appropriate Internet use and be given clear objectives for Internet use.

Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

7. How will Internet access be authorised?

The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.

All staff and pupils will have access to the Internet unless this is withdrawn.

Parents will be asked to sign and return a consent form when they are enrolled in to school and on entering KS2.

In general, pupils will not be issued individual email accounts, but will be authorised to us a group/class email address under supervision. Upper Key Stage 2 pupils may be provided with individual email addresses at the discretion of the class teacher and with written consent from parents. This will be closely monitored by the class teacher and will be withdrawn if used inappropriately.

In Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.

Parents will be informed that pupils will be provided with supervised Internet access.

8. How will filtering be managed?

The Technical Support Team (Oakford Technology) filters Internet access for pupils by cross-referencing all website requests against a banned list, which is continually updated. In addition to this, the school can permit or deny sites which are felt to be appropriate, for a chosen duration.

Staff have unrestricted access to the Internet such as for the purposes of downloading specific applications and accessing sites that are normally banned, e.g. viewing Youtube videos to use in the classroom environment. However, it is recommended that staff download such videos rather than showing them direct from the Youtube site..

A designated senior member of staff will review the sites accessed by the school. This is provided in weekly reports by the Technical Support Team (Oakford Technology) and other specific reports can be requested to investigate any issues that arise. The school will work in partnership with parents and Oakford Technology to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL and content must be reported to the Technical Support Team (Oakford Technology) via the Helpdesk. The

Computing Subject Leader must also be informed. (See section 17 for contact details).

At any time, the head teacher or Computing Subject Leader, may request a report from the Technical Support Team (Oakford Technology), listing all websites accessed from each individual device over an agreed time period.

9. How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Oakford Technology can accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

The head teacher will ensure that the e-Safety policy is implemented and compliance with the policy monitored.

10. Managing Content

10.1 How will pupils learn to evaluate Internet content?

Information received via the web, e-mail or text message requires good information-handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. Pupils need to understand that some content is deliberately misleading, while some is/may be unsuitable from purely a reading-age perspective.

If staff or pupils discover unsuitable sites, the URL and content must be reported to the Technical Support Team (Oakford) via the Helpdesk. (See Contact Details section).

Internet derived materials by staff and by pupils must comply with copyright law. Pupils are taught this as part of the Computing curriculum. Lessons will also teach pupils how to read for information from web resources, covering the validity of information and bias.

10.2 How should website content be managed?

The point of contact on the website is the school address, school e-mail and telephone number. Staff or pupils' home information is not be published.

Written permission from parents or carers is provided for all pupil photographs and names used on the school website. Where audio and video are included (e.g. Podcasts and Video Blogging) the nature of the items uploaded will not include content that allows the pupils to be identified.

11 Communication

11.1 Managing e-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

Whole-class or group e-mail addresses should be used at Key Stage 2, however, Year 6 may be given use of an individual email address to use within school if permission is given by parents. A code of conduct will also be signed by the class teacher, parent and pupil.

Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

11.2 On-line communications and social networking.

Where appropriate pupils will be taught about how to keep personal information safe when using online services and have specific computing lessons dedicated to e-Safety.

The school will conduct regular pupil surveys about home use of computing. It will gauge the range of activities which pupils undertake and how safely they are using them.

The use of online chat is not permitted in school, other than as part of its online learning environment.

11.3 Mobile technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones are not permitted within the school or on any school trip/residential. Pupils will be asked to give them to the Head teacher at the start of the school day. Staff must keep their personal mobile phones away from children in the class and they are only to be used away from the children (please refer to 'Laptop, computer and Internet policy for LM Staff).

11.4 Cyber-bullying

11.4.1 What is Cyber-bullying?

- Cyber-bullying is the use of computers and technology, commonly a mobile phone or the internet, deliberately to upset someone else.
- It can be used to carry out all the different types of bullying; an extension of face-to-face bullying.
- It can also go further in that it can invade home/personal space and can involve a greater number of people.
- It can take place across age groups and school staff and other adults can be targeted.
- It includes: threats and intimidation; harassment or 'cyber-stalking'; vilification/defamation; exclusion or peer rejection; impersonation; unauthorised publication of private information or images and manipulation.

11.4.2 Preventing Cyber-bullying

- All staff will be helped to keep up to date with the technologies that children are using.
- Pupils will be educated about cyber-bullying through a variety of means: assemblies, conferences, projects (Computing, PSHE, Drama, Literacy), Safer Internet Day etc.
- Parents will be provided with information and advice on cyber-bullying via literature, the school website etc.
- Pupils, staff and parents will be involved in evaluating and improving policies and procedures.

11.4.3 Reporting Cyber-bullying

- The Head teacher, designated member of staff for Child Protection, and designated Governor for Child Protection will:
    - Ensure staff can recognise non-verbal signs and indications of cyber-bullying. Publicise and promote the message that asking for help is the right thing to do and shows strength and good judgement.
    - Publicise to all members of the school community the ways in which cyber-bullying can be reported.

12 Introducing the Policy to Pupils

Rules for Internet access will be posted in all rooms where computers are used.

Where appropriate pupils will be taught about responsible Internet use and e-Safety will be included in the curriculum covering both school and home use.

Pupils will be informed that Internet use will be monitored.

13 Parents and E-Safety

Parents' attention will be drawn to the School E-Safety Policy.

Information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.

Internet issues will be handled sensitively to inform parents without undue alarm.

A partnership approach with parents will be encouraged.

14 Consulting with Staff and their inclusion in the E-Safety Policy

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.

The school's consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.

All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

Staff should be aware that Internet traffic is monitored and reported by Oakford Technology and can be traced to the individual user. Discretion and professional conduct is essential.

Community users of the school's Computing facilities are aware of the acceptable user policy before being granted access.

15 How will complaints be handled?

Responsibility for handling incidents will be delegated to a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

16 Web-based Resources

16.1 For Schools

KidSmart
http://www.kidsmart.org.uk/
SMART rules from Childnet International and Know It All for Parents

Childnet International
http://www.childnet-int.org/
Guidance for parents, schools and pupils

Becta / Grid Club, Internet Proficiency Scheme
On-line activities for Key Stage 2 pupils to teach e-safety.
http://www.gridclub.com/teachers/t_internet_safety.html

Kent Local Authority
http://www.clusterweb.org.uk/kcn/e-safety_home.cfm
Additional e-safety materials (posters, guidance etc.)

London Grid for Learning
http://www.lgfl.net/lgfl/sections/safety/esafety/menu/
Additional e-safety materials (posters, guidance etc.)

DfES Anti-Bullying Advice
http://www.dfes.gov.uk/bullying/

Prevent Duty guidance for England and Wales which relates to the Counter-Terrorism and Security Act 2015.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

Internet Watch Foundation
www.iwf.org.uk
Invites users to report illegal Websites

South West Grid for Learning – Safe
www.swgfl.org.uk/safe
A comprehensive overview of web-based resources to support schools, parents and pupils

Think U Know?
www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Wiltshire County Council – WISENET
Child protection advice relating to e-safety

16.2 For Parents

Kids Smart
http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents

Childnet International
http://www.childnet-int.org/
"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

Parental Control - Content Filters

http://www.vodafone.com/content/parents/howto-guides/content_filters.html

Parental Control - Controls on the Xbox

http://www.vodafone.com/content/parents/howto-guides/parental_controls_on_the_xbox360.html

Parental Control - Windows 7 Controls

http://www.vodafone.com/content/parents/howto-guides/windows_7_parental_controls.html

Parental Control - Google Safe Search

http://www.vodafone.com/content/parents/howto-guides/google_safesearch.html

Parental Control - YouTube Safety

http://www.vodafone.com/content/parents/howto-guides/youtube_safety_mode.html

Lydiard Millicent Primary School

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will only open or delete my own files on computers or any devices unless I am given permission to keep them.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- Any email messages I send will be polite and sensible.
- I understand that I must never give my personal details to anyone online or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately and use the 'e-Safety Problem' online form if I am able to.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or any computing devices.

Policy for responsible e-mail, network and Internet use for Lydiard Millicent School

1. I will use all Computing equipment in an appropriate way.
2. I will not:
   2.1. Access offensive website or download offensive material.
   2.2. Copy information from the Internet that is copyright or without the owner's permission.
   2.3. Place inappropriate material onto the Internet.
   2.4. Send e-mails that are offensive or otherwise inappropriate.
   2.5. Download files that could damage the device and school network.
   2.6. Access the files of others or attempt to change the computer settings.
   2.7. Update web pages, wikis or blogs etc. or use pictures and text that can identify the school, without the permission of the head teacher.
3. I will always log off the system when I have finished working.
4. I will always delete files that are no longer needed when I have finished using an iPad, iPod or similar device.
5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
6. My files should not be password protected by my own passwords. If I need to add a password to a document, I will arrange this with a teacher.
7. I will not use any removable media, such as a memory stick, without permission from a teacher.
8. I will not open e-mail attachments unless they come from someone I know.
9. . I will not use any joke emails or attachments.
10. I will report immediately to the Computing Subject Leader and / or the head teacher any unpleasant emails, or messages sent to me.
11. I understand that it is against the law to deliberately access Internet sites that contain certain illegal material.
12. I will not use the Internet for making money, gambling, political purposes or advertising is forbidden.
13. I will not tamper with school software or hardware in any way that could cause damage to the system,
14. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my access to all devices will be withdrawn and that other consequences may follow.

Lydiard Millicent Primary School - Guardian Letter

Date

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of Computing skills, Lydiard Millicent Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Our school technical support team, Oakford Technology operates a filtering system that restricts access to inappropriate materials and pupils are not allowed to use the internet without permission.

Due to the ever increasing pace of change within computing, we have recently updated and reviewed our E-safety Policy and Rules for Responsible Internet Use, which are available on the school website. Please would you read the attached rules with your children and sign and return the consent form in order to keep our records updated. Some of the points may not be relevant to the younger children of the school, however, please try to talk through them as much as you can.

Should you wish to discuss any aspect of Internet use please contact the school to arrange an appointment with the Computing subject leader or the head teacher.

Yours sincerely

Pupils' Consent Form

Lydiard Millicent

Responsible Internet Use

Please complete, sign and return to the school office.

Pupil:	***Class:***

Pupil's Agreement

I have read / understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed:	***Date:***

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.

Signed:	***Date:***
Please print name:	

Laptop, computer and Internet use policy for Lydiard Millicent school staff

1. The laptop remains the property of Lydiard Millicent School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Lydiard Millicent School Staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Lydiard Millicent School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the head teacher).
4. When in school and not being used, the laptop must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.
5. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the head teacher with evidence of adequate insurance.
7. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
8. Any software loaded must not affect the integrity of the school network.
9. If any removable media is used then it must be checked to ensure it is free from any viruses.
10. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up-to-date. Helpdesk can be consulted for advice on this.
11. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
12. Students must never use the laptop unless it is under the supervision of the teacher.
13. If any fault occurs with the laptop, it should be referred immediately to the Technical Support team via the Helpdesk.
14. When laptops are being transported, a carrying case should be used.
15. Staff will refrain from posting photographs of themselves of a sensitive nature or blog about school or work on any social media sites, or if they do ensure that they are not accessed by the public, by using password protection
16. Staff must not use personal mobile phones in class or in the playground areas whilst there are children or parents in view (mobile phones can be used on the staffroom, at the front of the school by the oak trees or their classroom out of school hours)
17. Personal cameras are not permitted in school unless by agreement with the head teacher
18. If children are photographed or videoed using a camera, iPad or similar device, that the images are only used for teaching and learning purposes at school unless parents agree that the images can be used on the school website or at other schools (cluster working)
19. If images are stored on a laptop or PC or tablet that is used at school and removed from school that the images are password protected or deleted
20. If staff access the school server at home for planning or teaching and learning purposes that they will not access any photographs or images of pupils (videos for example) unless they seek parental agreement

Useful contact details:

Oakford Technology Ltd – Technical Support Team - (including the registering of inappropriate content needing to be filtered).

Telephone: **01380 888088**

E-mail: lmihelpdesk@support.oakforduk.com

To notify of an inappropriate website:

lmihelpdesk@support.oakforduk.com

Notes on the Legal Framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day-to-day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of, amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following the signing of an agreement to use the equipment under the conditions as laid out by the school. (A copy of the Council's policy is included in section 15). The Rules for Responsible Internet Use, to which every user must agree, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring. For example, each school can review the websites visited by the school each day / week / month. Though this is not user specific it does allow a degree of monitoring to be conducted. All schools are also able to monitor school e-mail.

Cyber-stalking & Harassment

(http://wiredsafety.org/gb/stalking/index.html)

Under Section 1 of the Malicious Communications Act 1998 it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person and under Section 43 of the Telecommunications Act 1984 it is a similar offence to send a telephone message which is indecent, offensive or threatening. In both cases the offence is punishable with up to six months' imprisonment and/or a fine of up to £5000. As the Malicious Communications Offence is more wide-ranging than the Telecommunications offence it is more likely to be used by the Police than the Telecommunications Act offence.

In most cases involving malicious communications or cyber-stalking however there will be more than one offensive or threatening letter or telephone call and therefore the police will often choose to charge the offender with an offence contrary to Section 2 of the Protection from Harassment Act 1997; also punishable with up to six months' imprisonment. Part of the reason for using this charge is that when someone is convicted of an offence under the Protection from Harassment Act 1997 the court can make a Restraining Order preventing them from contacting their victim again. Breach of a Restraining Order is punishable with up to five years' imprisonment. A Restraining Order cannot be imposed for a conviction under the Malicious Communications or Telecommunications Acts.

If the e-mails, cyber-stalking etc. causes the victim to fear that violence will be used against them then the police can choose to charge the offender with an offence contrary to Section 4 of the Protection from Harassment Act 1997 which is punishable with up to five years' imprisonment and also allows the court to make a Restraining Order.

If the e-mails, cyber-stalking etc. is racist in nature or motivated by religious hostility then charges could be brought of Racially or Religiously-Aggravated Harassment contrary to Sections 32(1)(a) or 32(1)(b) of the Crime and Disorder Act 1998. If convicted offenders could face up to 7 years' imprisonment.

The fact that an offensive telephone call, letter e-mail etc. may be received in the course of work and have been sent by a work colleague or manager does not justify the message or prevent it being an offence. Offensive messages sent within the workplace can still constitute criminal offences. In addition they may justify a claim for constructive dismissal and compensation under employment law.

In many situations the recipient of malicious messages knows who the sender is. It may be a former partner or a relative which may mean that the victim is reluctant to involve the police. In those circumstances the victim could consider taking out an Injunction under Section 3 of the Protection from Harassment Act 1997. However we would always advise informing the police especially if the messages are in any way threatening. Even if the police decide not to prosecute they may give the offender a formal warning which could be used in evidence if they repeated their behaviour in future.

In addition to criminal prosecutions victims of harassment can sue the offender under Section 3 of the Protection from Harassment Act 1997 for damages arising out of the anxiety caused by the harassment and any financial loss it caused.

Glossary of Terms

Blog – Short for Web Log, an online diary

DCSF - Department for Children, Schools and Families

Podcast – a downloadable sound-recording that can be played on computers and MP3 players

Social Networking – websites that allow people to have "pages" that allow them to share pictures, video and sound and information about themselves with online friends

Video Blogging – online videos that can be uploaded via a web cam

Web 2 Technologies – a collection of online web services that are based around communicating/sharing information

URL – Uniform Resource Locator (web address)