DRAPERS' PYRGO PRIORY SCHOOL

Drapers' Pyrgo
Priory School

Online Safety Policy

Written: February 2017

Review: February 2018

Co-ordinator: Mr S Laurencin

Computing & ICT Technician: Mrs J Murphy

CONTENTS

1. Our Vision
2. Aims
3. Scope
4. Publicising e-Safety
5. Roles and Responsibilities
6. Physical Environment / Security
7. Communication
    - 7.1 Managing e-mail
    - 7.2 On-line communications and social networking.
    - 7.3 Mobile technologies
8. Educational Use
9. Digital Media
10. School Website
11. Educational Use
12. The use of the Internet to Enhance Learning
13. Responsibilities
    - 13.1 Pupil Responsibilities
    - 13.2 Staff Responsibilities
    - 13.3 Governor Responsibilities
14. Data Security / Data Protection
15. Equal Opportunities
16. Complaints
17. Raising Awareness of this Policy
18. Monitoring the Effectiveness of the Policy
19. References

- Web-based Rescources
- Sample letter to parents
- Pupil Acceptable User Agreement / e-Safety Rules
- Example Policy for responsible e-mail, network and Internet use for Pyrgo Priory Primary School.
- Notes on the Legal Framework

1. Our Vision

At Pyrgo Priory Primary School we believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curricular areas and associated communications technologies. The use of the Internet is an invaluable tool in the development of lifelong learning skills. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Pyrgo Priory aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

2. Aims

This policy document sets out the school's aims, principles and strategies for using the Internet and protecting pupils.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information, and communications with wider communities 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 pupils 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 pupils with quality Internet access as part of their learning experience.

Staff and pupils have access to web sites worldwide offering educational resources, news and current events. There will be opportunities for discussion and exchange of information within the school community and others worldwide. Staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the Local Authority and Department for Education (DfE); receive up to data information and participate in government initiatives such as National Education Network (http://www.nen.gov.uk/). The Internet is also used to enhance the school's management information and business administration systems.

3. Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults and young people while on the school premises

Related Documents:
Computing & ICT Policy
Acceptable Use Policy for Adults
Acceptable Use Policy for Young People
Data Protection Policy
Behaviour Policy
Anti-bullying Policy

4. Publicising Online Safety

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

- Make this policy, and related documents, available on the school website at: http://www.pyrgopriory.co.uk/
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant e-safety information in all areas where computers are used
- Provide e-safety information at parents' evenings, through the school newsletter, through the school website and social media.

5. Roles and Responsibilities

The Head and Governors have ultimate responsibility for establishing safe practice and managing Online Safety issues at our school. The Online Safety co-ordinator will be the central point of contact for all Online Safety issues however the responsibility for day to day management lies with the Computing co-ordinator.

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the Online Safety coordinator
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

6. Physical Environment / Security

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

- Anti-virus software is installed on all computers and updated regularly

- Central filtering is provided and managed by LGfL. All staff and students understand that if an inappropriate site is discovered it must be reported to the Online Safety co-ordinator who will report it the to LGfL Service Desk to be blocked. All incidents will be recorded in the Online Safety log for audit purposes.
- Requests for changes to the filtering will be directed to the Online Safety co-ordinator in the first instance who will forward these on to LGfL or liaise with the Head as appropriate. Change requests will be recorded in the Online Safety log for audit purposes
- All staff are issued with their own username and password for network access. Visitors / Supply staff are issued with temporary ID's and the details recorded in the school office
- All pupils in KeyStage 1 and 2 use individual logon ID's for their network access
-

7. Communication

7.1 Mobile / Emerging Technologies

- Teaching staff at the school are provided with an iPad for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.
- Staff understand that they should use their own mobile phones sensibly and in line with school policy.
- Pupils mobile phones should not be in school, if this occurs they should be turned off and handed into the school office on arrival for safe keeping.
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion
- Pictures / videos of staff and pupils should not be taken on personal devices but only on devices provided by the school.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

7.2. E-mail

Pupils must:

- only use approved e-mail accounts;
- report receiving any offensive e-mails;
- not divulge their or others personal details;
- not arrange to meet anyone via the e-mail or any form of social media;
- seek authorisation to send a formal e-mail to an external organisation
- not take part in sending chain letters

7.3 Social Networking and Personal Publishing

The school currently has a Facebook account and this is managed and updated by staff. Pupils are not allowed access to Social Networking Sites and these are currently blocked through the LGfL filtering system.

Guidance is provided to the school community on how to use these sites safely and appropriately. This includes

- not publishing personal information
- not publishing information relating to the school community
- how to set appropriate privacy settings
- how to report issues or inappropriate content

- Photographs published will not name any individual pupil

- Students' full names will not be published outside the school environment

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites

Staff are advised of the risks of putting private information into a public domain and also ‘bringing school into disrepute’ through the private use of social networking sites.

For the safety and the protection of all relevant parties: staff should NOT add/accept school pupils as friends on social networking sites.

9. Digital Media

We respect the privacy of the school community and will obtain written permission from staff; parents, carers or pupils before any images or video are published or distributed outside the school.

- Photographs published will not name any individual pupil
- Students' full names will not be published outside the school environment
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Students understand that they must have their teachers permission to make or answer a video conference call
- Supervision of video conferencing will be appropriate to the age of the pupils

10. School Website

The Head takes responsibility for content published to the school web site. Class teachers and Phase leaders are responsible for the editorial control of work published by their students.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses / staff e-mail addresses
- The school does not publish any contact details for the pupils or staff.

Contact details on the website will be:

- the school address
- e-mail address
- telephone number

The school website will not publish:

- staff or pupils contact details;
- the pictures of children without the written consent of the parent/carer;
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer

11. Educational Use

- School staff model appropriate use of school resources including the internet.
- Where appropriate, links to specific web sites will be provided instead of open searching for information. Pupils will be taught how to conduct safe searches of the internet as part of Computing lessons.
- Where pupils are allowed to freely search the internet e.g. using search engines, staff should be vigilant in monitoring the content of the websites the children visit.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity

- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of the information.

12. The Use of the Internet to Enhance Learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line 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.

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. The school 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 and Governors will ensure that the Internet policy is implemented and compliance with the policy monitored.

13. Responsibilities

13.1 Pupil Responsibilities

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. Online Safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies or lessons
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils and parents will sign the Internet/acceptable use policy (see appendix)
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils understand and follow the school E-safety and Acceptable Use Policy

- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- The pupil acceptable usage agreement will be displayed in the computer suite.
- Pupils will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access.

13.2 Staff Responsibilities

- Staff will ensure they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP). (See appendix)
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by the Senior leadership team.
- All staff need have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- Staff must report any suspected misuse or problem to the ICT Co-ordinator/ DSL/ E-safety coordinator or Head teacher for investigation / action / sanction
- Staff are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined as part of induction procedures.
- Computing Department staff will arrange annual e-Safety briefings for pupils, particularly for Yr5/6 and for secondary school transfer induction.

13.3 Governor Responsibilities

- Governors will be aware of this policy.
- Computing Link Governor will liaise with SLT to monitor annual e-Safety training for staff.

14. Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Process for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Data is stored on the school systems and transferred in accordance with the NAACE Data Security Guidelines

Staff must ensure that they:

- At all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data.

Sensitive personal pupil/staff data should never be taken off site without permission. In instances where permission is given, the personal data that is stored on personal computer systems, USB sticks or other removable media should adhere to the following:

- The data must be encrypted and password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device once it has been transferred or its use is complete.

15. Equal Opportunities

This e-safety policy works in conjunction with the school Equal Opportunities policy.

Responding to incidents

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, i.e.

- **Child sexual abuse images**
- **Adult material which potentially breaches the Obscene Publications Act**
- **Criminally discriminatory or prejudicial material**
- **Other criminal conduct, activity or materials**

- Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.
- Any suspected illegal activity will be reported directly to the police. The LGfL Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school;
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head;
- Breaches of this policy by staff will be investigated by the Head Teacher. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff;
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with school anti-bullying and child protection policies. There may be occasions when the police must be involved;

- Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with school Behaviour Policy. The Head Teacher will be made aware of – and may be asked to deal with - email alerts generated by PCE for students. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases;
- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school Behaviour policy;
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate

16. Complaints

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about Internet misuse by school personnel or pupils must be referred to the Headteacher.
- Parents will be informed if their child has misused the Internet.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be
- made to establish the legal position and discuss strategies.

17. Raising Awareness of this Policy

We will raise awareness of this policy via:

- the School Handbook/Prospectus
- the school website
- the Staff Handbook
- meetings with parents such as introductory, transition, parent-teacher consultations and periodic curriculum workshops
- school events
- meetings with school personnel
- communications with home such as weekly newsletters and of end of half term newsletters
- reports such annual report to parents and Headteacher reports to the Governing Body
- information displays in the main school entrance
- annual e-Safety briefings for pupils.
- Summer term Yr6 e-Safety refresher as part of Yr6/7 transition.

18. Monitoring the Effectiveness of the Policy

Annually (or when the need arises) the effectiveness of this policy will be reviewed by the coordinator, the Headteacher and the nominated governor and the necessary recommendations for improvement will be made to the Governors.

Headteacher:		**Date:**	
Chair of Governing Body:		**Date:**	

19. References

Web-based Resources

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/

Grid Club: http://www.gridclub.com/teachers/t_internet_safety.html

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:
http://wisenet.wiltshire.gov.uk/documents/dsweb/View/Collection-922

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.

Drapers' Pyrgo Priory School	**Name of School**	**Drapers' Pyrgo Priory School**
	AUP review Date	
	Date of next Review	
	Who reviewed this AUP?	

Acceptable User Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: LGfL StaffMail
- I will only use the approved email system with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Stephan Laurencin/Jan Murphy.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

- I will follow the school's policy on use of mobile phones / devices at school and will not take into classrooms / only use in staff areas.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using RM Portico and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Karen Becker, child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to Karen Becker or in her absence a senior member of staff.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- ***Staff that have a teaching role only:*** I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable User Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .....Date.....

Full Name ..... (printed)

Job title / Role .....

Drapers Pyrgo Priory School

KS1 Pupil Acceptable Use Agreement

Think before you click

S 

I will only use the Internet and email with an adult

A 

I will only click on icons and links when I know they are safe

F 

I will only send friendly and polite messages

E 

If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

Drapers Pyrgo Priory School

KS2 Pupil Acceptable Use Agreement

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

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 to7 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.