

Web-based Resources

For Schools

KidSmart

SMART rules from Childnet International and Know It All for Parents

<http://www.kidsmart.org.uk/>

Childnet International

Guidance for parents, schools and pupils

<http://www.childnet-int.org/>

Becta

e-Safety Advice

<http://schools.becta.org.uk/index.php?section=is>

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

Additional e-safety materials (posters, guidance etc.)

http://www.clusterweb.org.uk/kcn/e-safety_home.cfm

London Grid for Learning

Additional e-safety materials (posters, guidance etc.)

<http://www.lgfl.net/lgfl/sections/safety/esafety/menu/>

DfES Anti-Bullying Advice

<http://www.dfes.gov.uk/bullying/>

Grid Club

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

Internet Watch Foundation

Invites users to report illegal Websites

www.iwf.org.uk

South West Grid for Learning – Safe

A comprehensive overview of web-based resources to support schools, parents and pupils

www.swgfl.org.uk/safe

South West Grid for Learning – Filtering

<http://www.swgfl.org.uk/services/default.asp?page=filtering>

Think U Know

Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

www.thinkuknow.co.uk/

Wiltshire County Council – WISENET

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

For Parents

Kids Smart

A downloadable PowerPoint presentation for parents

<http://www.kidsmart.org.uk/parents/advice.aspx>

Childnet International

"Know It All" CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.

<http://www.childnet-int.org/>

Useful contact details:

South West Grid for Learning (SWGfL) Support Team - (including the registering of inappropriate content needing to be filtered).

Telephone: **0870 9081708**

E-mail: **support@swgfl.org.uk**

To notify of an inappropriate website: **abuse@swgfl.org.uk**

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.