West Hill School

E-Safety Policy

West Hill School supports a culture of whole school awareness, through policies, procedures and training that provide for a safe ICT environment.

Last Modified:
10/03/2011

West Hill School
E-Safety Policy

Contents

Document Control			
Version	Change	Author	Date
1.0	First Edition	Mrs L. Harrison Mr P. Gillon	March 2011

West Hill School
E-Safety Policy

1. Introduction

West Hill School supports a culture of whole school awareness, through policies, procedures and training that provide for a safe ICT environment.

The educational benefits of new and emerging technologies, such as the Internet and email, Virtual Learning Environments, weblogs, mobile phones, podcasting and video conferencing cannot be underestimated. These help to motivate children in their learning, equipping them with essential skills for the future, as well as enabling access to information which might not otherwise have been available.

Pupils and Staff might quite innocently happen upon inappropriate, offensive or illegal material on the Internet or, as is frequently highlighted in the media, unwanted contact might be received via text, email or in an online chat room. However, we cannot ignore the dangers associated with this emerging technology. Mobile phones, social networking sites or email might also be used by unscrupulous individuals to ‘Cyber Bully' peers or threaten and abuse members of staff.

West Hill School believes that the benefits far outweigh the risks involved so long as users are made aware of the issues and concerns and receive on-going education in choosing and adopting safe practices and behaviours.

E-safety is not an ICT issue. It may involve the use of ICT but it is about protecting children and young people from harm.

The E–Safety Policy is part of the School suite of ICT and Safeguarding Policies. It also relates to other policies including those for behaviour, anti-bullying, personal, social and health education (PSHE) and for citizenship.

The E-Safety Policy and its implementation will be reviewed annually. Our E-Safety Policy has been written by school to support the safe use of ICT through a culture of whole school awareness, utilising policies, procedures and training.

The school has appointed an E-Safety Team, consisting of:

- E-Safety Co-ordinator
- Child Protection Officer
- Network Manager
- Governor with Child Protection Responsibilities

2. Managing Information Systems

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

The school has a responsibility to ensure that ICT is used and managed legitimately, and the security of the school information systems and users will be reviewed regularly, as laid down in the school ICT Security Policy. *{Hyperlink}*

Published Content

The school makes use of both the school website and Life Channel TVs to promote and publish information about the school, its staff, pupils and events.

The publishing of content to these is limited to the ICT Support Team who vet the content prior to publication to ensure that it complies with school guidelines for publications including respect for intellectual property rights and copyrights.

Publication of Pupil Images and Work

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils are included. Nevertheless the security of staff and pupils is paramount.

To secure the safe management of the publication of pupil images and work, a number of strategies are identified and their application should be followed. Before the publication of any pupil image or material, permission must be sort from the Parent / Carer. In most instances permission is already granted through the pupil data collection sheet. You must check this before any publication is made. This is especially important where pupils are looked after children. This can be done through Data Manager, Network Manager or the Business Manager.

Photographs can be used providing no name can be linked to a particular student, i.e. a group photograph is taken and names are published but not in the order of the photograph. If a single photograph if used it is recommended that only the use of initial(s) and surname are published.

Further information can be found at:

www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/taking_photographs_in_schools.pdf

Social Networking, Social Media and Personal

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others. Please refer to the Staff Code of Conduct in the ICT User Guide. This states that IM and social networking is not acceptable with current or ex pupils under the age of 18. Breaches of this will be investigated and may lead to disciplinary procedures.

For the above reasons it has been decided that access to these sites in school will not permitted for all staff and pupils.

Emerging Technologies

Many emerging technologies offer the potential to develop new teaching and learning opportunities, including the use of mobile communications, Internet access, collaboration and multimedia tools.

The safety and effectiveness of these communications depends on users being trusted and identifiable. A risk assessment will be undertaken by the teacher and the E-safety team prior to use.

This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites such as Bebo, MySpace and Facebook. The registering of individuals to establish and maintain validated electronic identities, is essential for safe communication, but is often not possible.

3. Policy Implementation

This section summarises how the E-safety policy will be implemented across the school.

Internet Access

The internet and email facilities are provided to allow research to be conducted and as a means of communication with others access to these facilities is a privilege and not a right. Parental/carer consent is obtained via the pupil data collection. This allows the pupil to use the internet and e-mail and is confirmed each year by the agreement in the pupil planner.

Risk assessment

The school will take all reasonable precaution to ensure that users access only appropriate material. However, owing to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for material accessed or any consequences resulting from internet use.

However, school does employ the use of robust monitoring systems to reduce and manage the risks present. These are updated in accordance with industry guidelines.

The school will audit ICT use to establish that the e-safety policy is adequate and that the implementation is appropriate.

Handling of E-safety incidents

Minor incidents may be dealt with by a member of staff but should still be reported to the E-Safety team by phone and followed with an email for audit purposes. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy.

Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator and E–Safety Team. Advice on dealing with illegal use could be obtained from the Police and/or authorities. Please refer to the flow chart contained in this policy for additional guidance.

Cyberbullying

Cyberbullying is defined as:

The uses of ICT, particularly mobile phones and the internet, to deliberately hurt, embarrass or upset someone.

It is essential that young people, school staff and parents/carers understand how Cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying along with all forms of bullying will not be tolerated at West Hill School. Full details are set out in the schools Anti Bullying Policy. All incidences of Cyberbullying reported to the school will be recorded and investigated by the E-safety team.

Sanctions for those involved in Cyberbullying may include;

- The bully will be asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove content
- Internet access will be suspended for a period of time
- Computer access may be suspended for a period of time
- Parents/carers may be informed
- The police and Children's Social Care will be contacted if a criminal offense is suspected.

Repeat offences will lead to further sanctions as outlined in the anti-bullying policy.

DfE and Childnet have produced resources and guidance that can be used to give practical advice on Cyberbullying: http://www.digizen.org/cyberbullying.

Learning Platforms/environments

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, pupils, parents as well as support management and administration. It can enable pupils and teachers to collaborate in and across schools, can share resources and tools for a range of topics, create and manage digital content and pupils can develop online and secure e-portfolios.

The learning platforms/environments will be managed to allow only current staff, pupils and parents/carers access. All users should be aware that SLT and staff will monitor the usage of the learning platform in all areas, in particular message and communication tools and publishing facilities.

All users will be mindful of copyright issues and will upload only appropriate content onto the learning platform.

4. Communicating the policy

This policy has been designed with Governors, staff, pupils and parents/carers in mind. The contents of this should be shared with all these stakeholders and complied with.

It is important that all users feel confident to use ICT. The school E–Safety Policy will only be effective if everyone subscribes to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.

Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home.

Through the school website we provide parents/carers with information to help them to understand the risks involved and how to access a range of materials and other information to assist them. They can also contact the school for advice or to raise any concerns that they may have. These will be passed to the most relevant person for action.

5. Legal Framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently.

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.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

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). This can include images taken by and distributed by the child themselves (often referred to as “Sexting”).**A person convicted of such an offence may face up to 10 years in prison.**

The offence of grooming 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 asexual 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 (typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust) to engage in sexual activity with any person under 18.
Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Please refer to the “Children & Families: Safer from Sexual Crime” document included in the “Child Protection – Essential Guidance for all Staff” file located in the reception office.
More information about the 2003 Act can be found at www.teachernet.gov.uk

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
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

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 (email) 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 an author's "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.

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 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

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.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic".
Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

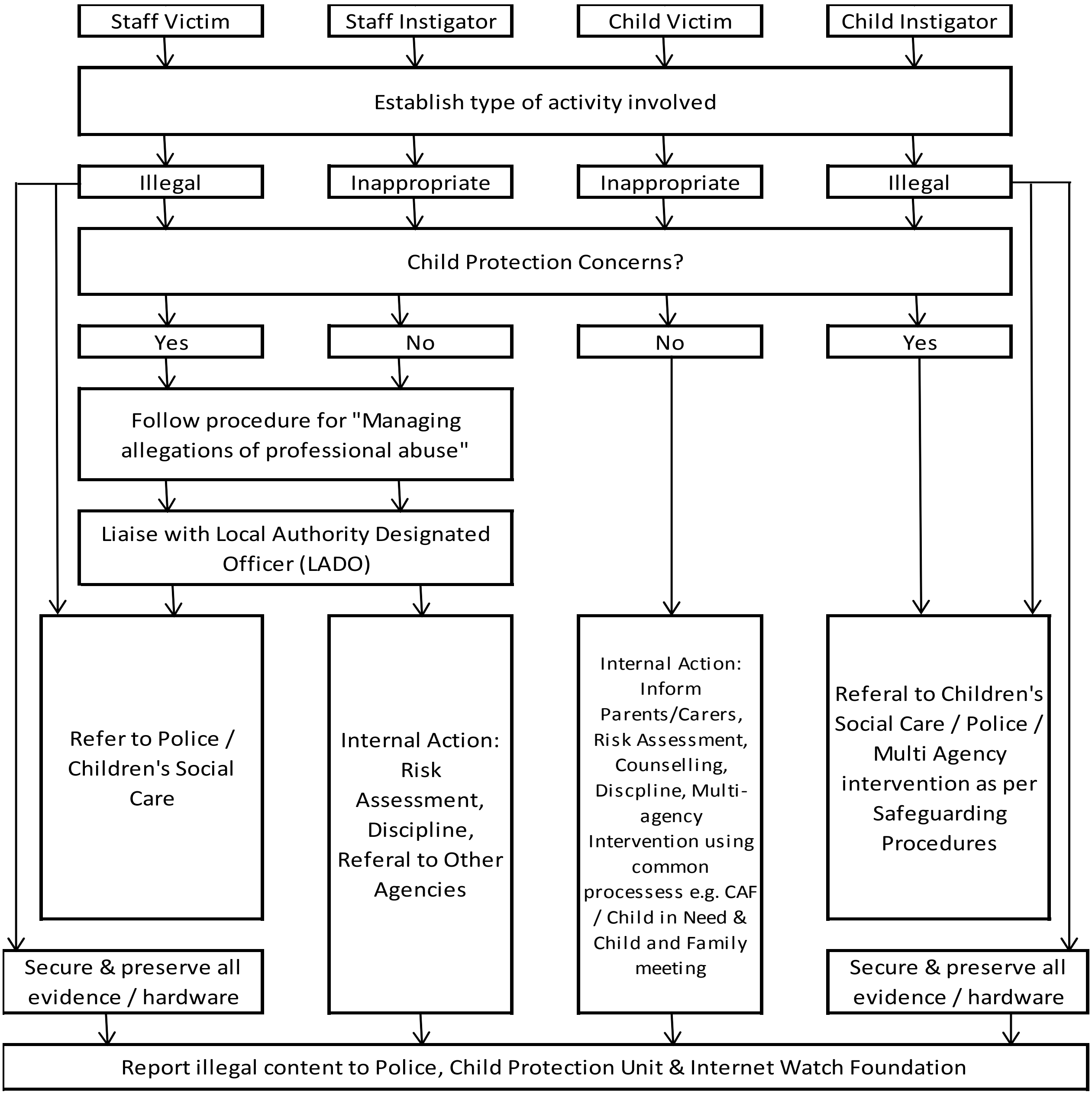
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:

Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
School staff are able to confiscate items such as mobile phones etc. when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

Telecommunications Act 1984

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

6. Reporting of incidents


Staff Victim
Staff Instigator
Child Victim
Child Instigator
Establish type of activity involved
Illegal
Inappropriate
Inappropriate
Illegal
Child Protection Concerns?
Yes
No
No
Yes
Follow procedure for "Managing allegations of professional abuse"
Liaise with Local Authority Designated Officer (LADO)
Refer to Police / Children's Social Care
Internal Action: Risk Assessment, Discipline, Referal to Other Agencies
Internal Action: Inform Parents/Carers, Risk Assessment, Counselling, Discpline, Multi-agency Intervention using common processess e.g. CAF / Child in Need & Child and Family meeting
Referal to Children's Social Care / Police / Multi Agency intervention as per Safeguarding Procedures
Secure & preserve all evidence / hardware
Secure & preserve all evidence / hardware
Report illegal content to Police, Child Protection Unit & Internet Watch Foundation