

Featherstone Wood Primary School



eSafety Policy

January 2014

Review Date Summer 2016

Contents

Introduction

Roles and Responsibilities

eSafety in the Curriculum

Password Security

Data Security

Managing the Internet safely

Managing other Web 2 technologies

Mobile Technologies

Managing email

Safe Use of Images

Misuse and Infringements

Equal Opportunities

Parental Involvement

Writing and Reviewing this Policy

Acceptable Use Agreement: Staff, Governors and Visitors

Acceptable Use Agreement: Pupils

Flowcharts for Managing an eSafety Incident

Incident Log

Smile and Stay Safe Poster

Current Legislation

Our e-Safety Policy has been written by the school, building on the Hertfordshire Grid for Learning exemplar policy (with acknowledgement to LGfL, SWGfL and Bristol City Council) and Becta guidance.

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:



Websites



Learning Platforms and Virtual Learning Environments



Email and Instant Messaging



Chat Rooms and Social Networking



Blogs and Wikis



Podcasting



Video Broadcasting



Music Downloading



Gaming



Mobile/ Smart phones with text, video and/ or web functionality



Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Featherstone Wood Primary School, we understand our responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, Governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought

onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in our school is Louise Shuttleworth, who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

Managing the school eSafety messages



We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.



The e-safety policy will be introduced to the pupils at the start of each school year.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.



Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

 Users are provided with an individual network and email log-in username.

 Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.

 Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school follows Becta guidelines (published Autumn 2008)

 Staff are aware of their responsibility when accessing school data. Level of access is determined by the Headteacher

 Data can only be accessed and used on school computers or laptops.
Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Hertfordshire Grid for Learning (HGfL)** is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

 The school continues to ensure that access to Internet resources (where reasonable) through the school's fixed and mobile internet technology is fully supervised

 Staff will preview any recommended sites before use.

 Raw image searches are discouraged when working with pupils.

 If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

 All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

 All users must observe copyright of materials from electronic resources.

Infrastructure

-  Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded.
-  School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to <http://www.thegrid.org.uk/eservices/safety/filtered.shtml>
-  Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
-  The school does not allow pupils access to internet logs.
-  The school uses management control tools for controlling and monitoring workstations.
-  If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator.
-  It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
-  Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.
-  If there are any issues related to viruses or anti-virus software, the network manager should be informed via the Headteacher.

Managing other Web 2 technologies

-  At present, the school endeavours to deny access to social networking sites to pupils within school.
-  All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
-  Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
-  Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests).

 Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

 Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

 Our pupils are asked to report any incidents of bullying to the school.

 Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other system approved by the Headteacher.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

 The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.

 All personal mobile devices **must** be switched off during teaching timetables. Staff expecting an urgent call can be contacted via the school office.

 The school is not responsible for the loss, damage or theft of any personal mobile device.

 The sending of inappropriate text messages between any members of the school community is not allowed.

 Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

 Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices (including phones)

-  The sending of inappropriate text messages between any members of the school community is not allowed.
-  Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
-  Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
-  Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

-  The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
-  It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
-  Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
-  E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
-  Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher, line manager or designated account.
-  Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
-  All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

 Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

 Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.

 Pupils are introduced to email as part of the ICT Scheme of Work.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

 With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

 Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked for permission to use their child's photos in the following ways:

 on the school web site

 in the school prospectus and other printed publications that the school may produce for promotional purposes

 recorded/ transmitted on a video or webcam

 in display material that may be used in the school's communal areas

 in display material that may be used in external areas, ie exhibition promoting the school

 general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa.
E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager has authority to upload to the site.

For further information relating to issues associated with School websites and the safe use of images in Hertfordshire schools, see

<http://www.thegrid.org.uk/schoolweb/safety/index.shtml>

<http://www.thegrid.org.uk/info/csf/policies/index.shtml#images>

Storage of Images



Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.



The Headteacher, has the responsibility of deleting images from the school network, when they are no longer required, or the pupil has left the school.

Webcams and CCTV



We do not use publicly accessible webcams in school.

For further information relating to webcams and CCTV, please see

<http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml>

Video Conferencing



At present video conferencing is not used at Featherstone Wood Primary School.

For further information and guidance relating to Video Conferencing, please see

<http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml>

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed (see appendix).

Inappropriate material

 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.

 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school. We consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

 Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website) when their child joins the school.

 The school disseminates information to parents relating to eSafety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website postings
- Newsletter item

Writing and Reviewing this Policy

Staff and pupil involvement in policy creation



Staff and pupils have been involved in making/ reviewing the eSafety policy through consultation and school council meetings.

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

This policy will be reviewed every 2 years and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.



Acceptable Use Agreement:

Staff, Governors and Visitors Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school eSafety coordinator.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without the permission of the Headteacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carers, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature Date

Full Name (printed)

Job title



Acceptable Use Agreement:

Pupils of Featherstone Wood Primary School

Agreement / eSafety Rules

- ✓ I will only use ICT in school for school purposes
- ✓ I will only use my class email address or my own school email address when emailing
- ✓ I will only open email attachments from people I know, or who my teacher has approved
- ✓ I will not tell other people my ICT passwords
- ✓ I will only open/delete my own files
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I know that my use of ICT can be checked and that my parent or carer contacted if a member of school staff is concerned about my eSafety



Featherstone Wood Primary School

Headteacher: Miss Louise Shuttleworth
Acting Chair of Governors: Mrs Michelle Gardner

Dear Parent or Carer,

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page.

If you have any concerns or would like some explanation please do not hesitate to contact me.

Yours sincerely,

Louise Shuttleworth
Headteacher

✂

eSafety Rules

We have discussed the eSafety rules and my child

.....

agrees to follow them and to support the safe use of ICT at Featherstone
Wood Primary School.

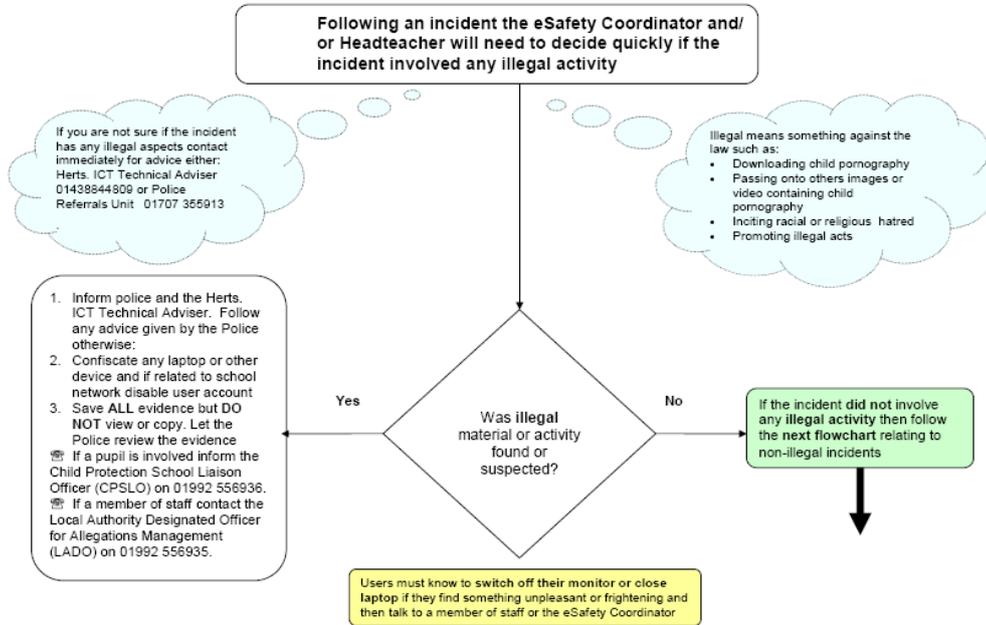
Signed : Relationship :

Year Group: Date:.....

Flowcharts for Managing an eSafety Incident

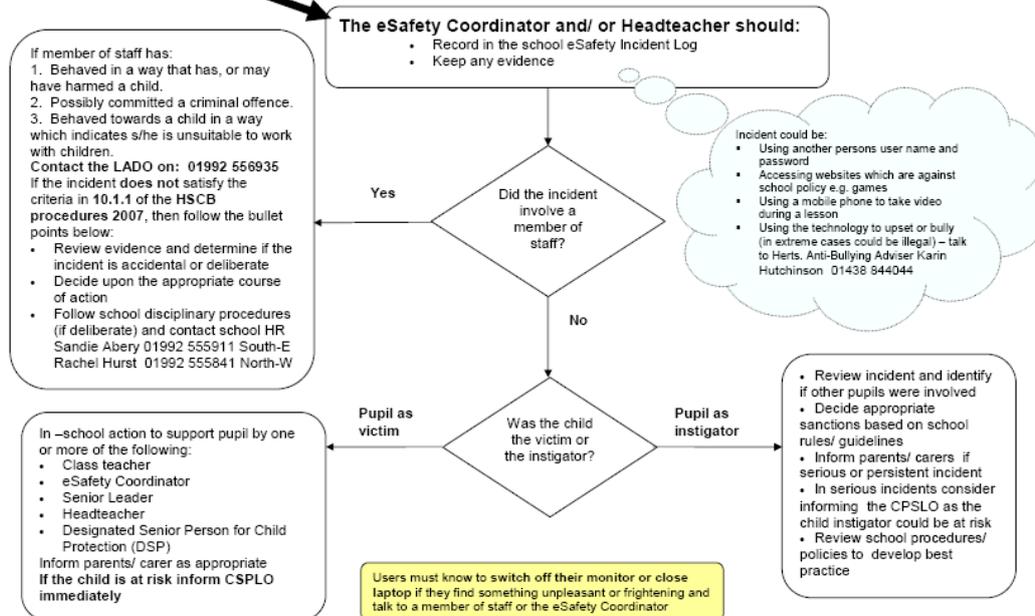


Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident For Headteachers, Senior Leaders and eSafety Coordinators



If the incident did not involve any illegal activity then follow this flowchart

Hertfordshire Managing an eSafety Incident Flowchart For Headteachers, Senior Leaders and eSafety Coordinators



Integrated Bullying and Racist Incident Record

For each incident please complete one form and return to the designated teacher for collation and monitoring.

1. Focus of Bullying/Harassment

Please tick all elements which apply in your understanding of the incident(s):

	Definitely applies	Possibly applies
Ability		
Age/ Maturity		
Appearance		
Class/Socio-economic		
Learning Difficulties and Disability		
Ethnicity/Race*		
Religion/Belief*		
Institutional Racism*		
Gender		
Homophobia		
Sexualised		
Size		

*See County Guidelines on Dealing with Racist Incidents

2. Manifestations of Bullying/Harassment (indicate those that apply)

Perception of individual: feelings of being bullied/harassed	
Isolation/ignoring	
Teasing	
General expressions of prejudice/stereotype	
Racist literature, graffiti or insignia	
Verbal abuse or name calling (specify below)	
Targeted graffiti or hurtful note writing	
Threats including threatened physical assault	
Mobile phone/text message bullying/harassment	
Internet related bullying/harassment	
Camera phone bullying/harassment	
Actual physical assault	
Other:	

3. Those involved – please record where appropriate:

- adults as targets or perpetrators (A)
- perpetrators from outside the school community (O)

Targeted/wronged/distressed person/s (including ethnicity and other relevant diversity issues)	Person/s giving offence (including ethnicity and other relevant diversity issues)

4. Description of incident(s)
 Please give a precise account including places, date, times and any witnesses.
 Attach any further information (e.g. pupils' accounts, witness accounts, notes of meetings)
 N.B. Indicate if it is a repeat incident.
 N.B. indicate if a serious incident referral should be made to the LA.

5. Action taken:
 Please record all steps (including meetings, letters, investigations, sanctions)

6. Summary of those notified and/or involved

(Delete italic options where applicable)	✓	Any details (e.g. dates)
Head Teacher		
Chair of Governors		
<i>Form tutor/class teacher</i>		
Head of Year		
'Target' parents/carers informed school by <i>letter/telephone/in person</i>		
'Target' parents/carers notified by <i>letter/telephone/in person</i>		
'Target' parents/carers invited to the school		
'Offending person/s' parents/carers informed school by <i>letter/telephone/in person</i>		
'Offending person/s' parents/carers notified by <i>letter/telephone/in person</i>		
'Offending person/s' parents/carers invited to the school		
Local Authority: SEA/SIP, Bully advisor or MECSS		
Police		
Others (specify):		

7. Date for monitoring progress of those involved. Follow up on the incident and check that all parties are progressing well academically and socially

Date.....

8. Reporting member of staff:

Name

Date

Smile and Stay Safe Poster

E-Safety Rules to be displayed next to all PCs in school



SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, instant messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making 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.

<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information

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.

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 another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. 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. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.