



---

**SAINT PIUS X  
CATHOLIC HIGH SCHOOL**

**A SPECIALIST SCHOOL IN HUMANITIES**

# ICT Acceptable Use Policy and Guidance

Our Mission Statement:

“Saint Pius X Catholic High School is a Catholic School  
in which the Gospel message of the Kingdom of God  
is revealed through our work and through the relationships  
we establish with our brothers and sisters in Christ”

Originator: Susan Smith, Deputy Head teacher January 2011  
Noted by Governing Body Asset Management Committee January 2011  
Date of next review: December 2011

# Contents

- Introduction
- Aims of this policy
- What is an AUP?
- Who's responsible?
- Protocols
  - Data security
  - Passwords
  - Email
  - Internet
  - Mobile technologies
  - Other web 2.0 technologies
  - Images
  - Behaviour and respect
- **Equal opportunities**
- **Reviewing the policy**

## Appendices

- A: Acceptable Use Agreement: Staff
- B: Acceptable Use Agreement: Key Stage 3 and 4
- C: Flowchart for Managing an eSafety Incident
- D: Incident Log
- E: Current Legislation
- F: Glossary of terms used
- G: Further information and guidance

# Introduction

In order to exploit the many educational and social benefits of new and emerging technologies, learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. Schools are increasingly recognising the benefits of technology and particularly Web 2.0 technologies as an essential component of productive and creative social learning.

eSafety is about enabling an institution to benefit as much as possible from the opportunities provided by the Internet and the technologies we use in everyday life, not just about the risks, and how we avoid them. It is about ensuring everyone has the chance to develop a set of safe and responsible online behaviours that will reduce the potential risks but still allow access to the benefits. Acceptable Use Policies (referred to as AUPs throughout this document), help to promote the positive behaviours needed. Any incidents that may arise will be dealt with quickly and according to policy to ensure students and staff are protected.

The school will endeavour to safeguard against all risks, but may never be able to completely eliminate them all.

A glossary is provided at Appendix (F) which may help to explain some of the more unfamiliar terms used throughout this policy.

## Aims of this policy

This policy is designed for use by students and all staff in Saint Pius X Catholic High School.

Essentially, the key priorities are to:

- ensure the safeguarding of all students within and beyond the educational setting by detailing appropriate and acceptable use of all on-line and off-line technologies.
- outline the roles and responsibilities of everyone involved.
- ensure everyone is clear about procedures for misuse of any on-line and off-line technologies both within and beyond the educational setting.
- develop links with parents and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues.

## AUP

AUP is an acronym for **Acceptable Use Policy**, a document which sets out the way in which users of ICT should and should not make use of the systems provided to them, including connectivity to the Internet, for example, knowing what is polite to write in an email to another user or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

End user AUPs for students are included within the student diary and for staff are found within the staff planner. They are also displayed in prominent locations in the vicinity of

ICT environments. The AUPs can be found in the appendices at the end of this document (A, B).

# Responsibilities

It is the overall responsibility of the Headteacher with the support of the Governing Body and staff to ensure that there is an overview of eSafety (as part of the wider remit of Child Protection) across the school and to implement this policy.

## Staff and other adults

It is the responsibility of all adults within the school to:

- Ensure that they know who the designated person for Child Protection is within the school so that any misuse or incidents which involve a student can be reported. Where an allegation is made against a member of staff it should be reported immediately to the appropriate person, either the Child Protection Officer, Line Manager or Headteacher.
- Be familiar with the Behaviour Management, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed.
- Ensure that students are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner in order to be in control and know what to do in the event of an incident.
- Be up-to-date with eSafety knowledge that is appropriate for the age group and reinforce this through the curriculum.
- Sign the Acceptable Use Policy in the staff planner to demonstrate that they agree with and accept the rules for staff and other adults using ICT.
- Use ICT in an appropriate way that does not breach the Data Protection Act 1998.

## Children and young people

It is the responsibility of all students within the school to:

- Follow the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new student attends the school for the first time.
- Use the Internet in a safe and responsible manner following teaching through ICT, PSHE or other clubs and groups.
- Have the confidence to inform an adult about any inappropriate materials or contact from someone they do not know immediately.

## Parents

Parents can play a vital role in supporting this policy with their child, which is demonstrated by discussing and signing the AUP end user agreement together so that it is clear to the school that the rules are accepted by the child or young person with the support of the parent. (There is no statutory requirement for parents to sign AUP end user agreements but evidence shows that children and young people signing agreements to take responsibility for their own actions, is successful). The AUP is also intended to provide support and information to parents when children and young people may be using the Internet beyond school.

A useful guidance publication for parents has been produced by Becta:  
<http://publications.becta.org.uk/display.cfm?resID=41513>

## Local Safeguarding Children's Board (LSCB)

Both Rotherham's LSCB and Children's Board will support all children, young people, their parents and the children's workforce to ensure the safety of children and young people when they are using ICT and related technologies.

There is a requirement to deliver a single clear approach to pro-actively addressing eSafety with a coherent and unified strategy to managing it. A sub group of the LSCB has been established (eSafety Sub Group) and will ensure that best practice is shared, developed and implemented across the whole of Rotherham.

Please refer to the LSCB eSafety Strategy for Rotherham 2008-11 for further information:  
[Insert link here](#)

## Protocols

### Data Security

Personal information is defined by the fact that an individual could be identified from that information. This could be name, address, date of birth, telephone numbers and images which, in isolation, may not be of concern and would not necessarily identify an individual, but, by amalgamating several data items, may do so and therefore disclose their personal details. If personal details are not kept secure, this may lead to that individual becoming exposed to risks such as fraud, theft and even their personal safety could be compromised.

The Data Protection Act 1998 contains 8 enforceable principles of good practice which the school will adhere to at all times when using, storing, accessing and sharing personal information. Personal information will be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary

- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

Further information about the Data Protection Act 1998 can be found in Rotherham Borough Council's [Data Protection Policy](#):

- It is important that users do not access folders and files on a computer or network area that they do not have permission to use. The Computer Misuse Act 1990 makes it an offence to access material without the system owner's permission.
- Before attempting to plug in portable media devices, permission must be sought from the Network Manager. Devices such as digital cameras, flash drives, CDs/DVDs, mobile phones and MP3 players may contain viruses that could be a potential threat to a computer or network.
- If images of other users are being used (a media project for example) care must be taken not to save onto any personal device without either the permission of the individual. If these devices are ever stolen or lost, someone's personal information may be disclosed to unknown individuals.

Other sources of information on data security:

Information Commissioner's Office – 'Security of personal information':

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/security%20v%201.0\\_plain\\_english\\_website\\_version1.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security%20v%201.0_plain_english_website_version1.pdf)

BECTA - "Good practice in information handling" guide:

[http://schools.becta.org.uk/index.php?section=lv&catcode=ss\\_lv\\_saf\\_se\\_03&rid=14734](http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_se_03&rid=14734)

The following link provides a useful test to check that the information held is 'personal information' according to the Data Protection Act 1998:

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/160408\\_v1.0\\_determining\\_what\\_is\\_personal\\_data\\_-\\_quick\\_reference\\_guide.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/160408_v1.0_determining_what_is_personal_data_-_quick_reference_guide.pdf)

## Passwords

- Students and staff are provided with a unique individual network, email and Learning Platform log-in username and password. These are of the length and complexity recommended by Becta.
- It is important to ensure that any passwords are kept private and not shared. If the network is accessed and used inappropriately by someone pretending to be you, it may mean that you could be held responsible for any actions as it will be difficult to prove it wasn't you. Do not write passwords down.
- If you think that someone knows your password and has used it to access the network, report this to the Network Manager immediately.
- It is good practice to be responsible with your personal log-in details which will help you be vigilant when using other systems including your home environments.

- It is also good practice to log off when you have finished your session or when you need to move away from the computer. Try to get into the habit of doing this each time you leave the computer so that no one else can use your settings. It's only a small inconvenience to log back in again.

## Email

- Staff are provided with their own email account to use for all educational business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed to anyone else.
- It is the responsibility of each email account holder to keep the password secure. For the safety and security of users and recipients, all email is filtered and logged; if necessary email history can be traced.
- Under no circumstances should staff contact students or parents or conduct any work related business using personal email addresses e.g. contacting students about homework should only be via a school e-mail address, not a personal one, to safeguard staff from misunderstandings or allegations.
- All email users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission.
- Students may only use approved email accounts on the network and only under direct supervision (where appropriate) for educational purposes.
- The forwarding of chain letters is not permitted. Any other type of email received that appears to be inappropriate or of concern should be referred to the line manager.
- RGfL provides a standard disclaimer that is attached to all email correspondence as follows:

*The information in this e-mail is confidential and intended solely for the use of the individual to whom it was addressed. If you are not the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please advise the sender by using the reply facility in your e-mail software, and then delete it from your system. Rotherham Schools may monitor the content of the e-mails sent and received via its network for the purposes of ensuring compliance with the law and with Rotherham schools policies. Any views or opinions presented are only those of the author and not those of Rotherham Schools.*

Essentially, the above statement protects the email account holders' organisation from inappropriate use by the user and helps to prevent any unnecessary unauthorised use of any outgoing email by intended or unintended recipients.

## Internet

Both this policy and the AUP end user agreement are inclusive of both fixed and mobile internet technologies: desktop PCs, laptops, notebooks, netbooks, personal digital assistants (PDAs), tablets, webcams, interactive whiteboards, voting systems, digital video equipment etc. and technologies owned by students and staff such as laptops, mobile phones, digital cameras, PDAs and portable media players, etc.

- The school will not monitor staff except in specific situations where misconduct or misuse is suspected. However, all use of the RGfL network and other similar networks is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be investigated.
- Students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff should preview any recommended sites before use.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by a member of staff. It is advised that parents recheck these sites and supervise this work where this is practical or reasonable.
- All users must observe software copyright at all times. It is illegal to copy or distribute software or illegal software from other sources.
- All users must observe copyright of materials including text and images.
- If staff or students discover an unsuitable site, this should be reported immediately to the Network Manager.
- 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 ICT equipment.
- Users are not permitted to download programs or files without seeking prior permission from the Network Manager.
- If there are any issues related to viruses or anti-virus software the Network Manager should be informed.

## Mobile technologies

- Staff and other adults are allowed to bring in personal mobile phones for their own use, but these should not be used within lessons. Under no circumstances should a member of staff contact a student or parent using their personal device. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Students are not allowed to bring in personal mobile devices/phones without express permission from the Headteacher or other delegated member of staff. The

breaking of this school rule is dealt with in the Behaviour Management policy and procedures.

- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate or threatening text messages between any members of the community is not allowed and will constitute a serious offence.
- 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 or other adults, this device may be only used to conduct educational business outside of the educational setting.

## Other Web 2.0 technologies

At present, access is denied to social networking sites to staff and students unless a clear business need has been granted. (Staff may only create blogs, wikis or other web 2.0 spaces in order to communicate with children and young people using the Learning Platform or other systems that have been approved).

- All staff and students are advised to be cautious about the information given by others on sites e.g. users not being who they say they are.
- Images of yourself, family, friends or colleagues on such sites (or details within images that could give background details) should be avoided and the appropriateness of any images posted considered carefully due to the difficulty of removing once online.
- Personal details which may identify you and your whereabouts (full name, address, mobile/home phone numbers, school details, email address, specific hobbies/interests, etc.) should not be given on such sites.
- It is advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Users are encouraged to be wary about publishing specific and detailed private thoughts online.
- Any incidents of bullying or material or instructions you are uncomfortable with should be reported to the appropriate member of staff.

For further advice and guidance about social networking:

<http://www.ico.gov.uk/youth.aspx>

## Images

- With the written consent of parents, (on behalf of students) appropriate capturing of images by staff and other students is permitted.
- Staff and students are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students or staff. This includes when on field or residential trips. However, with the express permission of the Headteacher or other designated staff, images can be taken provided they are transferred immediately and solely to the network and deleted from the device.

Further guidance on the use of images in educational settings:

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/taking\\_photos\\_v3.0\\_final.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/taking_photos_v3.0_final.pdf)

### Consent of adults who work at a school

- Permission to use images of all staff who work at the school should be sought on induction and a copy should be located in the personnel file.

### Publishing student images and work

Parents are asked to give permission to use their child's work/photos in the following ways:

- on a web site
- on a Learning Platform
- in a prospectus and other printed publications
- recorded/transmitted on a video or webcam
- in display material that may be used in communal areas
- in display material that may be used in external areas, e.g. exhibitions
- general media appearances, e.g. local or national media/press releases, etc

The consent form is considered valid for the entire period that the child attends the school unless there is a change in circumstances. Parents may withdraw permission, in writing, at any time. Names will not be published alongside their image and vice versa unless prior permission is sought. Email and postal addresses will not be published particularly alongside images in connection with the individual.

### School website (if different to the Learning Platform space)

The uploading of images to a school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission is always sought from the parent prior to the uploading of any images.

### Webcams, video conferencing and CCTV

- Webcams are only ever used for specific and direct learning purposes
- Misuse of webcams by any member of the community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
- Where webcams are used, consent will be sought from parents and staff in the same way as for all other images.

Rotherham MBC CCTV Policy and Guidance:

<https://public.rgfl.org/esafety/Information%20Governance/Forms/AllItems.aspx>

## Behaviour and respect

### Behaviour and Anti-Bullying Policies

The Anti-bullying policy contains the procedures for dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. All behaviours are seen and dealt with in exactly the same way, whether on or off-line.

Any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any members of staff or students about a member of staff should be reported to the Child Protection Officer, Line Manager or Headteacher. In the event of an allegation being made about the Head teacher it should be reported to the Chair of Governors.

### External websites

If a member of staff finds themselves or another adult victimised on an external website, such as 'Rate My Teacher', they are encouraged to report this to the Headteacher and their union.

### Disciplinary Procedure for All Staff

Breaches of behaviour and good conduct through misuse of on-line technologies will be dealt with via the school's disciplinary procedures.

### Complaints

Complaints relating to eSafety should be made to the Headteacher or Line Manager. The flowchart for managing incidents should be followed (see Appendix C). Incidents should be logged (see Appendix D).

## Equal Opportunities

Staff are aware that some children and young people may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of ICT acceptable use issues.

### Overcoming potential barriers for individuals and groups

To overcome potential barriers staff will, for example, have to take into consideration the following specific needs of students, and how these might affect their approaches to learning:

- Special Educational Needs (e.g. Asperger Syndrome, Dyslexia, Dyspraxia, ADHD, general learning difficulties, etc.)

- Difficulties with communication, language and literacy
- Behavior difficulties
- Physical impairment
- Emotional difficulties
- English as an additional language (EAL)
- Race and ethnicity
- Religious belief
- Gender issues
- Social background
- Ability.

In conclusion, equal opportunities, and inclusive practice in school involves careful planning by all professionals concerned to ensure effective learning opportunities for all students.

A range of resources on accessibility and access to learning can be found on the Becta website:

[http://schools.becta.org.uk/index.php?section=tl&catcode=ss\\_tl\\_inc\\_ac\\_03&offset=0&rows=10&orderby=1](http://schools.becta.org.uk/index.php?section=tl&catcode=ss_tl_inc_ac_03&offset=0&rows=10&orderby=1)

## Implementing this policy

- Staff, students and parents will have access to this policy on the school website and the Rotherham Portal site.
- AUPs will be included in the staff planner and student diary annually.
- A record that staff have signed the AUP will be kept.
- A record that students have signed the AUP will be kept.
- Copies of AUPs will be placed in strategic positions around the school at the start of each academic year.

## Reviewing the Policy

### Review Procedure

- There will be an on-going opportunity for staff and students to discuss any issue of eSafety that concerns them.
- This policy will be reviewed every 12 months and consideration given to any comments or suggestions for future versions.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.
- Staff and students will be actively encouraged in reviewing the policy through staff meetings or School Council for example.

- APPENDIX A

# ICT Acceptable Use Policy

## For staff and visitors

This policy is designed to ensure that all staff and visitors are aware of their responsibilities when accessing and using any form of ICT. All staff and visitors are expected to sign this agreement and adhere to its contents at all times.

- I will only use ICT and any related technologies for professional purposes or for uses deemed 'reasonable' by the school, Governing Body or Line Manager/Supervisor
- I will comply with ICT security policies and not disclose any passwords provided to me by the school or other related educational settings.
- I will ensure that all electronic communications with Children and Young People and staff are compatible with my professional role.
- I will not give out my own personal details, such as a mobile phone number and personal email address to children and young people.
- I will only use the approved email system(s) for any work related business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off site or accessed remotely. Personal data can only be taken off site or accessed remotely when authorised by the school, Governing Body or Line Manager.
- I will not install any hardware or software without prior permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of children and young people and/or staff will only be taken, stored and used for professional purposes inline with any policy and with prior written consent of a parent, school or Line Manager.
- 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 the school, Governing Body or Line Manager.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both business and private environments, will not bring my professional role into disrepute.
- I will support and promote the Acceptable Use Policy and help children and young people and adults 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

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

Full Name ..... (Please print)








Job title .....

# ICT Acceptable Use Agreement

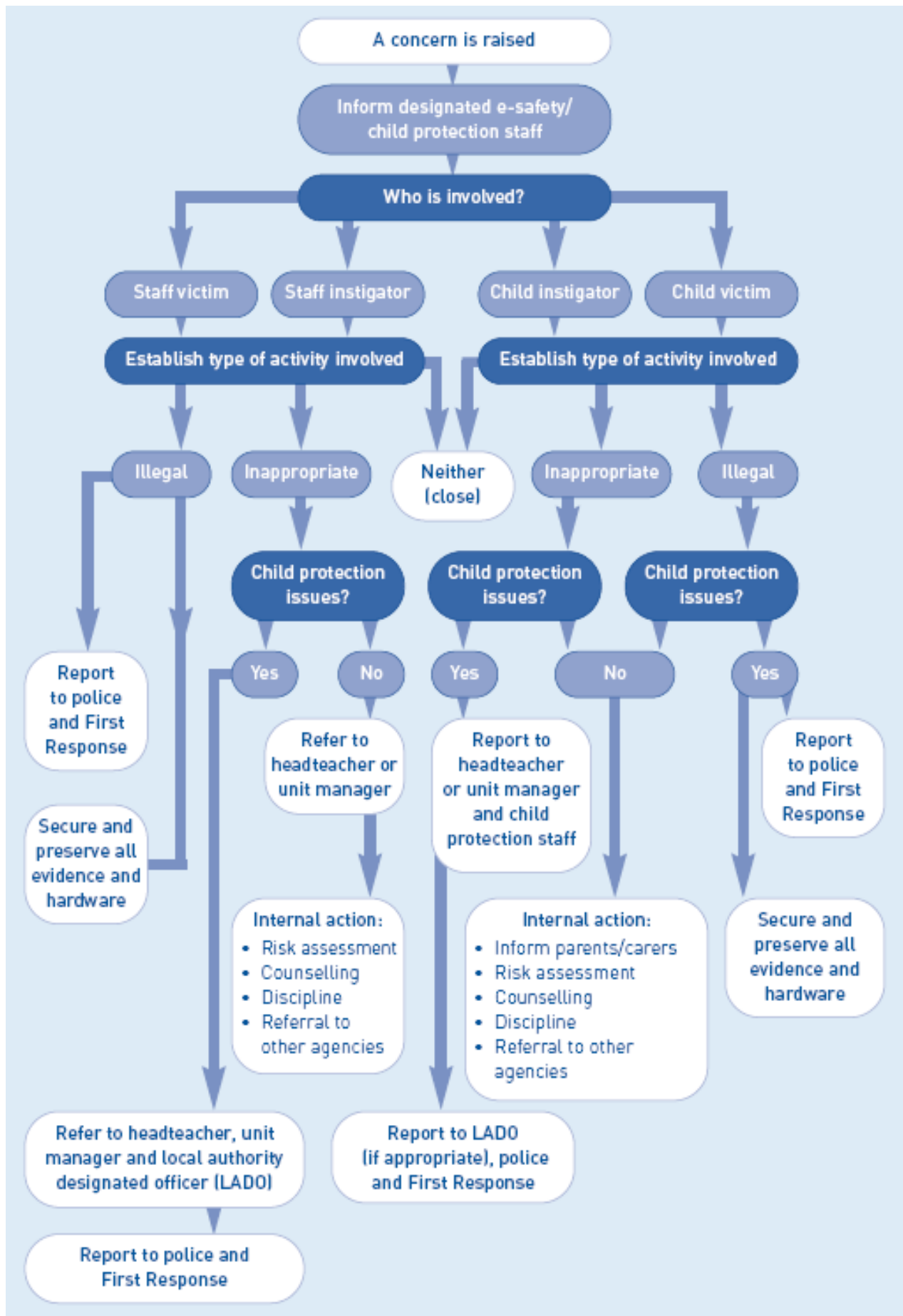


All ICT users must read and follow the conditions set out in this agreement. If you need help or are unsure about anything written below, please ask a member of staff or refer to the main policy which supports this agreement. Any breach of the conditions below may lead to withdrawal of your access to ICT and the network.

Policy link

<p><b>Passwords</b></p> 	<ul style="list-style-type: none"> <li>• I will only use my own ID and password to log onto a computer.</li> <li>• I will not give out my password to anyone.</li> <li>• I will log off properly after I have finished with the computer.</li> </ul>	
<p><b>Email</b></p> 	<ul style="list-style-type: none"> <li>• I will not access or create any material that may cause upset to others.</li> <li>• If I am unsure about opening or downloading any attachments or contents of an email, I will ask a member of staff.</li> <li>• I will not send abusive or threatening language in an email to others.</li> </ul>	
<p><b>Data Security</b></p> 	<ul style="list-style-type: none"> <li>• I will keep my personal information safe from other people.</li> <li>• I will not access any other user's files and folders without permission.</li> <li>• I will not use portable media (like memory sticks) on the network without asking a member of staff first.</li> </ul>	
<p><b>Internet</b></p> 	<ul style="list-style-type: none"> <li>• I will not browse or download anything illegal and forward or share any material that could cause upset to anyone.</li> <li>• If I do come across any such material I will report it immediately to a member of staff.</li> <li>• I will not attempt to bypass the internet filtering system.</li> <li>• I will not attempt to access any unsupervised/unauthorised chatrooms or areas.</li> </ul>	
<p><b>Images</b></p> 	<ul style="list-style-type: none"> <li>• I will only take, store and use images of children, young people and/or staff for an agreed project or purpose.</li> <li>• I will only use images outside the network if I have permission from the people in the image and a member of staff.</li> <li>• I will only use images that have been approved by a member of staff.</li> </ul>	
<p><b>Behaviour</b></p> 	<ul style="list-style-type: none"> <li>• I will only communicate with others online sensibly.</li> <li>• I will not send or encourage others to send abusive messages.</li> <li>• I will make sure that any online or offline activity will not cause the school/centre, staff and any other user, distress or embarrassment.</li> </ul>	
	<ul style="list-style-type: none"> <li>• I know that all use of the network is monitored if abuse is suspected.</li> <li>• I will treat other people and ICT equipment with care and respect.</li> <li>• It is my responsibility to respect and follow all of the above conditions which will help to keep me and other's safe while using ICT.</li> </ul>	

# Flowchart for managing an e-safety incident



APPENDIX D

# Incident Log

Date of incident:	
Member of staff reporting incident:	
URL, (web address) of incident:	
Copy of screens/evidence saved to:	
Location of incident (room):	
Computer number if known:	
Details:	
Passed to:	
Action taken	

## APPENDIX E

# Current Legislation

### Acts relating to monitoring of individuals

#### Data Protection Act 1998

The Act requires anyone who handles personal information to comply with 8 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.hms0.gov.uk/acts/acts1998/19980029.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 RIPA 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.hms0.gov.uk/acts/acts2000/20000023.htm>

#### Human Rights Act 1998

<http://www.hms0.gov.uk/acts/acts1998/19980042.htm>

### Other Acts relating to eSafety

#### Racial and Religious Hatred Act 2006

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.

#### 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.

#### Crime and Disorder Act 1998

<http://www.opsi.gov.uk/acts/acts1998/19980037.htm>

## 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 sex 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 sex Crime*" document as part of their child protection packs. For more information: [www.teachernet.gov.uk](http://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 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.

## 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.

Privacy and Electronic Communications (EC Directive) Regulations 2003  
(Including spam)

<http://www.opsi.gov.uk/si/si2003/20032426.htm>

# Glossary

Some of the following phrases and acronyms are found within this policy. There are others that do not appear but may serve as a useful reference:

**API:** Acronym for Application Program Interface, a set of tools, routines and rules for building software applications in a consistent way.

**Asynchronous Learning:** Mode of learning event in which participants are not online at the same time and are unable to communicate without time delay.

**Authentication:** Process of confirming the identity of an individual.

**AUP:** Acronym for Acceptable Use Policy i.e. agreed procedures in place to minimize e-security and e-safety risks

**AVI:** Acronym for Audio Video Interleave - the file format used by Microsoft Video for Windows.

**Bandwidth:** Term that describes how much data can be sent via a connection in a specified time. This measurement is typically described in bps or bits per second.

**Becta:** British Educational Communications and Technology Agency - A Government funded agency promoting use of ICT.

**Bit:** The minimum unit of computer data - either a 0 or a 1.

**Blog:** A blog (a contraction of the term "web log") is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

**Bps:** Acronym for Bits per second the units in which the speed of modems are rated. Indicates the amount of information a modem can transmit and receive each second.

**Browse:** Process of viewing web pages over the World Wide Web.

**Browser:** Program that allows you to view and interact with web pages on the World Wide Web.

**Byte:** Unit for measuring data - usually 8 bits.

**CEOP:** The Child Exploitation and Online Protection Centre - delivers a multiagency service dedicated to tackling the exploitation of children.

**CD:** Acronym for Compact Disc. Originally an audio-only format the CD has spawned a range of derivatives including CD-ROM (Compact Disc Read Only Memory), CDi (Compact Disc Interactive) CD-R (CD-ROM Recordable) and most recently CD-RW (Compact Disc Read Write).

**Chat:** Talking to one person or many people, usually in text format via the internet.

**Childnet:** A non-profit organisation working with others to help make the Internet a positive and safe place for children and young people.

**Compression:** Reducing the size of a file so that it can be transmitted more quickly and takes up less storage space.

**Cookie:** Small element of data sent to your computer when you visit a website. When you subsequently return to the site, this data may be used for a range of things including recalling your username.

**DHTML:** Acronym for Dynamic HTML - a new way of developing web pages with enhanced functionality. Standards for DHTML are still being developed.

**Digital:** Made up of zeros (0) and ones (1) or bits of information

**DNS:** Acronym for Domain Name System - the system that regulates naming of computers on the internet. The core of the system is a vast database that stores the names and network addresses of every computer, accessed whenever a computer needs to convert a Domain Name into a numeric IP address.

**Domain:** Official name for a computer attached to the Internet. Email addresses normally consist of a user ID and a domain name separated by the @ symbol.

**Download:** The process of copying files from one remote host to your computer, usually via FTP.

**DVD:** Acronym for Digital Versatile Disc

**E-Learning:** Wide range of electronic learning applications and processes including Web-based learning, computer-based learning, virtual classrooms and digital collaboration. Commonly held to include delivery of content via the Internet, intranet, extranet (LAN/WAN), audio, video tape, satellite broadcast, interactive TV and CD-ROM.

**Email:** Sending electronic messages over a network or the internet.

**E-Security:** Procedures to ensure all electronic data is categorised as public, restricted or protected and that electronic systems containing the data are securely maintained.

**E-Safety:** procedures to ensure computer users know their access rights and responsibilities in using ICT.

**Extranet:** A local area network (LAN) or wide area network (WAN) using HTML, SMTP, only available to people inside and certain people outside an organization, as determined by the organization.

**FAQ:** Acronym for Frequently Asked Questions.

**Flash:** A vector graphic animation tool marketed by Macromedia and widely used for developing web delivered e-learning.

**FTP:** Acronym for File Transfer Protocol. A process that allows you to transfer files or programmes to or from computers across the internet.

**GIF:** Acronym for Graphics Interchange Format - a common format for the storage of largely non-photographic imagery.

**Gigabyte:** 1024 megabytes of computer data.

**Hardware:** Physical technology such as computers, monitors and keyboards rather than software.

**Hits:** The number of requests for information made to a server.

**Host:** Computer that exists to allow other computers to connect with it.

**HTML:** Acronym for Hypertext Mark-up Language - the basic language that is used to construct web pages. There are several HTML standards in existence, the latest of which is HTML 4.

**HTTP:** Acronym for Hypertext Transfer Protocol, the standard that regulates the way information is transferred around the World Wide Web.

**Hyperlink:** Underlined word or set of words that, when clicked, takes you to a different place on that page or to a new destination altogether.

**ICT:** Acronym for Information and Communication Technology.

**Internet:** The full range of networks interconnected via internet protocol.

**IP:** Acronym for Internet Protocol, the rules that regulate the way information is transferred across the Internet.

**IPS:** Acronym for Intrusion Prevention System - a network security device that monitors network and/or system activities for malicious or unwanted behaviour and can react, in real-time, to block or prevent those activities.

**ISP:** Acronym for Internet Service Provider - companies that provide users with access to the internet.

**Intranet:** A private network inside an organisation that uses Internet technology, but is segregated from the Internet by a firewall. This means that authorised users can only access this network.

**ISDN:** Acronym for Integrated Services Digital Network. This telecommunications technology provides increased bandwidth using telephone lines but generates significant additional cost.

**Java:** Language developed specifically for creating software that can be simply downloaded from the Internet, but now used for a wide range of applications.

**Javascript:** Language similar to Java but actually incorporated into web pages in the interests of creating various special effects.

**JPEG:** Acronym for Joint Photographic Experts Group - the committee that originally developed this special image file format. JPEG files are now the most popular format for storing photographic images.

**Kilobyte:** Unit of computer data, made up of 1024 bytes.

**Learning Platform:** A Virtual Learning Environment (VLE) with facilities for communication, work storage and access to learning resources.

**Learning Portal:** A website that offers learners consolidated access to learning and training resources from multiple sources.

**Login:** The action involved in entering a computer system or the account name you have been authorised to gain access to a system with.

**Megabyte:** Unit of computer data made up of 1024 kilobytes.

**MIS:** Acronym for Management Information System - provides a co-ordinated approach to the gathering and use of data.

**Modem:** Device that allows one computer to connect to another via a telephone line.

**MPEG:** Acronym for Moving Picture Experts Group - the committee who devised this innovative file format for storing video images.

**Network:** Two or more computers connected together.

**Network Manager:** Someone who oversees the network, monitoring its performance, security, error detection and who implements access controls.

**Offline:** Term that implies that an item of hardware or software is no longer actively linked with the Internet. See Online below.

**Online:** Opposite of Offline - i.e. an item of hardware or software is actively linked with the Internet.

**Operating System:** The basic system that underpins computer operations and the foundation upon which all other programs operate. MSDOS, UNIX and Windows are all examples of operating systems.

**Plug-in:** Small pieces of software that add to the capability of existing programs.

**PDA:** An acronym for personal digital assistant - a mobile device or palmtop computer.

**POP:** Acronym for Post Office Protocol or Point of Presence - the location where connections to a network or the Internet may be accessed via dial-up networking

**Remote Access:** Accessing and/or processing data from a computer in a different location.

**Router:** Mechanism for transferring data between one or more networks.

**Server:** Both the software and hardware that is used to provide access to an internet resource.

**SIRO:** Acronym for Senior Information Risk Owner - a senior manager who co-ordinates and takes responsibility for action related to e-security and eSafety.

**SMTP:** Acronym for Simple Mail Transport Protocol. The standard that governs how email is sent and received.

**Software:** The files, data and programs that allow a computer to function but have no physical dimensions. By way of contrast, see 'Hardware'.

**Terabyte:** Unit for a vast amount of computer data, consisting of 1024 gigabytes.

**Twitter:** This is a free social networking and micro-blogging service that enables its users to send and read messages known as tweets. Tweets are text-based posts of up to 140 characters displayed on the author's profile page and delivered to the author's subscribers who are known as 'followers'.

**Upload:** Send files to another computer, usually via FTP.

**URL:** Acronym for Universal Resource Locator otherwise known as the address of a website.

**VoIP:** Acronym for Voice over Internet Protocol - or using the internet to transmit voice conversations, a technique increasingly used within virtual classroom systems.

**Virus:** Self-replicating software that propagates itself from one computer system to another, normally devised with malicious or mischievous motives.

**VLE:** Acronym for Virtual Learning Environment (See Learning Platform)

**VPN:** Acronym for Virtual Private Network which is a software application to create a private computer link between computers in different locations.

**Web space:** Amount of data capacity available for the construction of web pages, normally measured in megabytes.

**Website:** Collection of linked web pages with a common theme, created for the same purpose.

**World Wide Web:** A global information resource made up of interconnected web pages.

**Glossary courtesy of Bedfordshire County Council**

# Further Information and Guidance

The nature of e-safety and technology is evolving rapidly. You may wish to keep up to date with further supporting documents, information or advice, which can be found on:

- [www.parentscentre.gov.uk](http://www.parentscentre.gov.uk) (for parents)
- [www.ceop.co.uk](http://www.ceop.co.uk) (for parents and adults)
- [www.iwf.org.uk](http://www.iwf.org.uk) (for reporting of illegal images or content)
- [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) (for all children and young people with a section for parents and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- [www.netsmartkids.org](http://www.netsmartkids.org) (Suitable for 5 – 17 year olds)
- [www.kidsmart.org.uk](http://www.kidsmart.org.uk) – (Suitable for all under children under 11 years)
- [www.phonebrain.org.uk](http://www.phonebrain.org.uk) (for Years 5 – 8)
- [www.bbc.co.uk/cbbc/help/safesurfing](http://www.bbc.co.uk/cbbc/help/safesurfing) (for Years 3 and 4)
- [www.hectorsworld.com](http://www.hectorsworld.com) (for Foundation Stage, Years 1 and 2 and is part of the thinkuknow website above)
- [www.teachernet.gov.uk](http://www.teachernet.gov.uk) (for schools and other educational settings)
- [www.digizen.org.uk](http://www.digizen.org.uk) (for materials from DCSF around the issue of cyberbullying)
- [www.becta.org.uk](http://www.becta.org.uk) (advice for educational settings to update policies)
- <http://www.nextgenerationlearning.org.uk/esafetyandwifi.html> (simple tips for parents / adults)
- <http://www.rscb.org.uk/Home.aspx> (Rotherham Safeguarding Children’s Board – policies, procedures and practices.
- [www.nen.org.uk](http://www.nen.org.uk) (for schools and other educational settings – access to the National Education Network)
- <http://www.yhgfl.net/> Yorkshire and Humber Grid for Learning – Regional broadband consortium currently with 13 member Local Authorities signed up.
- [http://www.rotherham.gov.uk/info/442/librariescomputers\\_and\\_the\\_internet/601/computers\\_and\\_the\\_internet/2](http://www.rotherham.gov.uk/info/442/librariescomputers_and_the_internet/601/computers_and_the_internet/2) - Rotherham Borough Council Libraries Service – Computers and the internet, on-line safety advice.