Rotherham Metropolitan Borough Council
Where Everyone Matters

Children & Young People's Services

Acceptable Use Policy
for schools and other educational settings

Policy & Guidance 2010/11

Rotherham Safeguarding Children Board

South Yorkshire POLICE

National Education Network

YH GfL Yorkshire & Humber GRID FOR LEARNING

Contents Page

- **Section 1: Introduction** **5**
- **Section 2: Aims of this policy** **7**
- **Section 3: What is an AUP?** **8**
- **Section 4: Why are AUP's important?** **9**
- **Section 5: Who's responsible?** **10**
- **Section 6: AUP themes** **13**

Passwords 13
Email 14
Data security 15
Internet 16
Mobile technologies 18
Social Networking / web 2.0 technologies 19
Images 20
Webcams, video conferencing and CCTV 22
Video hosting sites 22
Behaviour and respect 23

- **Section 7: Managing an eSafety incident** **25**
- **Section 8: Equal opportunities** **26**
- **Section 9: Writing and reviewing this policy** **28**

Appendices

A: Acceptable Use Agreement: Staff, Governors and Visitors **29**
B: Acceptable Use Agreement: Key Stage 1 and 2 **30**
C: Acceptable Use Agreement: Key Stage 3 and 4 **34**
D: Flowchart for Managing an eSafety Incident **38**
E: Incident Log **39**
F: Current Legislation **40**
G: Glossary of terms used **43**
H: Further information and guidance **48**

Disclaimer

Every effort has been made to take into account relevant laws and best practice in the preparation of this publication. However, eSafety issues have the potential to be complex and multi-faceted and, as case law in this area is still very much under development, nothing in this publication should be deemed to constitute legal advice.

If you have a specific query relating to eSafety practice in your organisation, you should seek help from an appropriate adviser which may include the Local Authority (LA), or Local Safeguarding Children Board (LSCB), child protection experts, the Police, the Child Exploitation and Online Protection (CEOP) Centre, the Internet Watch Foundation (IWF), counsellors, legal advisers, the Department for Education (DfE) or others.

Rotherham MBC (and other contributors to this document) can therefore accept no liability for any damage or loss suffered or incurred (whether directly, consequentially, indirectly or otherwise) by anyone relying on the information in this publication or any information referred to in it. Inclusion of resources or references in this publication does not imply endorsement by Rotherham MBC (or other contributors), nor does exclusion imply the reverse.

URL's and information given in this document were correct at the time of publication, but may be subject to change over time.

Important

Rotherham MBC's educational network including Internet and email provision is, in most part, connected to Rotherham Grid for Learning (RGfL).

Rotherham MBC are considered to be a 'connected organisation' and as such, form part of a Regional Broadband Consortium (RBC) which has a direct feed into the Yorkshire and Humber Grid for Learning (YHGfL) network or 'Grid'. The Grid is provided by the YHGfL Foundation Limited who is responsible for running and managing the Grid.

It is a condition of the YHGfL Foundation Limited that any connecting organisation (including Rotherham MBC) must ensure that its employees and all users of the Grid are aware of all the conditions laid down in both this Acceptable Use Policy and the YHGfL Acceptable Use Policy.

The YHGfL Acceptable Use Policy can be found on their website at:
http://www.yhgfl.net/About-Us/YHGfL-AUP

Version control and history

Version	Date of Revision	Amended by	Notes
0.1	March 2009	James Keeley	First draft
0.2	November 2009	James Keeley	Second draft
0.3	January 2010	James Keeley	Third draft
0.4	February 2010	James Keeley	Fourth draft following review from stakeholders
0.5	May 2010	James Keeley	Fifth draft – final amendment to wording
0.6	May 2010	James Keeley	Sixth draft – additional wording and formatting
0.7	May 2010	James Keeley	Seventh draft – formatting completed
0.8	June 2010	James Keeley	Eighth draft – formatting completed
0.9	June 2010	James Keeley	Ninth draft – New comments added
1.0	29 June 2010	James Keeley	Final version created

Section 1 Introduction

In 2008, Dr Tanya Byron (now Professor) produced an independent review to help parents and their children get the most from new technologies whilst protecting children from inappropriate or harmful material. The focus was on internet safety and video games.

Following the reviews recommendations, there has been a lot of good work around eSafety and this is expected to continue following Professor Byron's 2010 progress report.

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. At times, they will encounter risks.

We now recognise, however, that eSafety risks are posed more by behaviours and values online than the technology itself. Our approach must therefore change: rather than restricting access to technology, we need to empower learners to develop safe and responsible online behaviours to protect them whenever and wherever they use technology. Acceptable Use Policies (referred to as AUP's throughout this document), when embedded within a wider framework[1] of eSafety measures, can help to promote the positive behaviours needed.

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. It's not just about the risks, and how we avoid them; it's about ensuring everyone has the opportunity to develop a set of safe and responsible behaviours that will enable them to reduce the risks but still access the benefits.

[1] Becta's **PIES model:**
(Policies, Infrastructure, Education and Standards)

Schools and other establishments are increasingly recognising the benefits of technology and particularly social networking as an essential component of productive and creative social learning. However, in doing so, they are finding that a 'blocking and banning' approach which merely limits exposure to risk is no longer a sustainable approach. Ofsted's recommendation is that learning environments move towards 'managed' systems with fewer inaccessible websites. This should be accompanied by teaching and learning that equips children and young people to manage online space positively and safely.

Children and young people will experiment online, and while their confidence and enthusiasm for using new technologies may be high; their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter. Educational establishments now need to focus on a model of **empowerment**: equipping children and young people with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they use technology.

Section 2 Aims of this policy

This policy is designed for use by children and young people and their parents, Head teachers, Governing Bodies, eSafety coordinators, Child Protection Officers and other staff in an educational environment in the first instance.

This policy has been written as a guide for all schools and other educational settings, where many eSafety risks and management issues are the same, with the same key messages for children, young people, their parents, staff and other users.

It is the responsibility of the individual establishment to adapt the content of this policy to their needs and curriculum whilst still reflecting the key messages and procedures required to successfully implement this policy.

Essentially, the key priorities of this policy are:

- To serve as a supplement and reference to the AUP posters.
- To ensure the safeguarding of all children and young people within and beyond the educational setting by detailing appropriate and acceptable use of all online and offline technologies.
- To outline the roles and responsibilities of everyone involved.
- To ensure everyone is clear about procedures for misuse of any online and offline technologies both within and beyond the educational setting.
- To develop links with parents and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues.
- To educate children, young people and parents about using ICT and the internet in a safe & responsible way.

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

Section 3 What is an AUP?

AUP is an acronym for Acceptable Use Policy; at its most basic level, it is a document usually in the format of a poster which sets out the way in which users of ICT should and should not make use of the systems provided to them, including using the Internet. AUP posters should be displayed in prominent locations in the vicinity of ICT environments, notice boards, website or Intranet.

Contained within this policy and guidance, are three grades of an AUP poster. You should choose one that is appropriate to the age group of the intended user. These can be found in the Appendix; at A, B or C.

Appendix A is intended for the school workforce, (including Governors) and visitors, staff in other youth settings and libraries. In other words, any adult with supervisory capacity where they have access to ICT in which children and young people also have access to. These are generally not displayed as a poster but should be signed by the adult and retained on file for reference.

Appendix B is intended for children of a 'primary school' age (5-11years or Key Stage 1/2) who have access to ICT within a learning environment. This is not necessarily restricted to a school setting and therefore will be appropriate to display in youth centres or cafes and libraries for example. It has been designed specifically with the age of the end user in mind. That is to say, it is informative without appearing to be threatening or heavy handed in its approach. A copy of both the AUP and signatory page (which forms part two of the AUP), should be given to the end user so that they are able to share and discuss with a parent before both parent and child signs and returns part two.

Appendix C is intended for children and young people of a 'secondary school' age (11-16 years or Key Stage 3/4) who have access to ICT within a learning environment. Again, this is not necessarily restricted to a school setting and therefore will be appropriate to display in youth centres or cafes and libraries for example. It has been designed specifically with the age of the end user in mind. Whilst some end users of secondary age possess enhanced knowledge and skills in ICT, the AUP is designed not to be too formal and threatening in nature. A copy of both the AUP and signatory page (which forms part two of the AUP), should be given to the end user so that they are able to share and discuss with a parent before both parent and child or young person signs and returns part two.

It is envisaged that introducing the concept of eSafety by sharing and discussing the AUP with parents will provide and insight into a child or young person's involvement with ICT and to help recognise the dangers as well as the benefits.

Section 4 Why are AUP's important?

AUP's demonstrate how work has been achieved to create a balance between using ICT to enhance learning and teaching, and putting appropriate safeguards in place at the same time.

AUP's are an important way of encouraging all members of the community to take responsibility for their own safety when using technology. Effective AUP's can help to establish and reinforce safe and responsible online behaviours both in an educational environment as well as in the home where many inappropriate behaviours go undetected.

AUP's are also an effective means of protecting an organisation by ensuring that all users of ICT are aware of the consequences and actions of inappropriate behaviour or malicious intent. AUP's are also designed to protect staff from any unwarranted accusations from either staff or children and young people. For example, some staff may be unaware that contacting or responding to a child or young person through personal channels (such as a private social networking account) is inappropriate which could lead to investigation, either as an internal matter by their employer and / or the Police. The AUP should therefore provide clear guidance in this respect.

Section 5 Who's responsible?

eSafety is an important aspect of strategic leadership within the educational setting and key stakeholders have ultimate responsibility to ensure that policy and practices are embedded and monitored.

This policy, supported by the AUP's for staff, Governors, visitors and children and young people is available to protect the interests and safety of the whole learning community.

Schools and other educational settings

It is the overall responsibility of Head teachers 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 schools and to implement this policy or an adaptation of it.

Staff and other adults

It is the responsibility of all adults within a school or other educational setting to:

- Ensure that they know who the designated person for Child Protection is within the school or other setting so that any misuse or incidents can be reported which involve a child or young person. Where an allegation is made against a member of staff it should be reported immediately to the nominated Child Protection Officer and recorded.

- Be familiar with Behaviour, Anti-bullying (including cyberbullying) and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately.

- Ensure that children and young people are protected and supported in their use of online and offline technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.

- Be up-to-date with eSafety knowledge and be equipped with eSafety training skills (where applicable) that are appropriate for the age group and reinforce this through the curriculum.

- Sign an AUP to demonstrate that they agree with and accept the rules for staff and other adults using ICT. All staff should receive a copy of the AUP which must be signed and retained on file. The AUP should be displayed in a prominent area (e.g. Staff Room) to serve as a reminder that staff and other adults have an equal responsibility in the safe use of ICT.

- Use ICT in an appropriate way that does not breach the Data Protection Act 1998 and other relevant and associated legislation.

Children and young people

Children and young people should be actively encouraged to become involved in the review of this policy through a School Council or other similar forum, in line with this policy being reviewed and updated.

In addition, children and young people should be;

- Responsible for following the AUP rules whilst within an educational setting commencing from the beginning of each academic year or whenever a new child or young person attends a school or similar setting for the first time.

- Taught to use the Internet (including mobile phones that can access the Internet) in a safe and responsible manner through ICT, PSHE, clubs and groups, Citizenship or collapsed timetable days on eSafety.

- Taught to have the confidence to inform an adult about any inappropriate materials or contact from someone they do not know immediately, without reprimand (age and activity dependent).

The AUP and the accompanying letter for children and young people and parents are provided in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school and other educational settings.

The AUP is specifically designed to help children and young people understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. 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 encountering unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The AUP should be prominently displayed within the school or similar setting and especially in an ICT suite, where appropriate, so that it provides a constant message at all times.

Parents

Parents can play a vital role in supporting this policy with their child, which is demonstrated by discussing and signing the AUP together so that it is clear to the school or setting, 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's but evidence shows that children and young people signing agreements to take responsibility for their own actions, is largely successful.)

The AUP is also intended to provide support and information to parents when children and young people may be using technology beyond an educational setting (i.e. Home environment).

Furthermore, it is hoped that parents will contribute to future amendments or updates to this policy so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents feel should be addressed, as appropriate. Educational learning environments are encouraged to promote eSafety

through family sessions which will provide an opportunity for parents to raise any issues or concerns they may have.

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

The UK Council for Child Internet Safety (UKCCIS) has launched a useful 'Click Clever, Click Safe' Code designed to act as an everyday reminder of simple good behaviours, to help parents and their children avoid common risks online:
http://clickcleverclicksafe.direct.gov.uk/index.html

Rotherham Safeguarding Children Board (RSCB)

Both RSCB and Rotherham 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 using ICT and related technologies.

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

Please refer to RSCB for further information: http://www.rscb.org.uk/Home.aspx

Section 6 AUP themes

Each of the following sub headings in this section are specifically designed to support and compliment the AUP posters by providing additional guidance.

Passwords

It is recommended that this standardised password policy is adopted in line with BECTA standards:

Length	Complexity	Lifespan (staff)	Lifespan (students)
8	Yes	90 days	365 days

- Depending upon the age group and setting, users may be provided with a unique individual network, email and Learning Platform log-in username and password.
- It is important to ensure that any passwords belonging to users are kept private and not shared with anyone else. Passwords should never be written down.
- If a user suspects that their password has been accessed and has been used by someone to access the network, this should be reported to a member of staff immediately.
- Likewise, passwords must never willingly be shared with anyone else. If the network is accessed and used inappropriately by someone pretending to be another user, it may mean that the default user could be held responsible for any actions as it will be difficult to prove misuse otherwise.
- It is good practice for users to be responsible with their personal log-in details which will help them to remain vigilant when using other systems including home environments.
- It is also good practice to end a session by logging off correctly or when temporarily moving away from the computer. Users should attempt to get into the habit of doing this each time the computer is left unattended so that no one else can use the open session. It is only a small inconvenience to log back in again.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of networks and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users or administrators must also make sure that workstations are not left unattended and are locked.

eMail

The use of email within most environments is an essential communication tool for adults, children and young people. Educationally, email can offer significant benefits. For example; direct written contact between establishments on different projects, be they staff based or pupil based, within school, national or international.

It is recognised that all email users need to understand how to style an email appropriate to their skills, experience, age and understanding.

All users provided with an email account should follow these basic principles of good practice guidelines and in line with school or other educational setting's policies:

- Staff are usually 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 their 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 children and young people or parents or conduct any work related business using personal email addresses.

- Rotherham Grid for Learning email (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 example 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.

- Email sent to an external organisation should be written carefully and professionally before sending. An email is a record in the same way that a letter is written on headed paper. The same rules apply equally to emails sent internally.

- 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 discussed with a member of staff.

- 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 from an adult.

- Staff must inform an eSafety coordinator or Line Manager/Supervisor if they receive an offensive email.

Data Security

Personal information is defined by the fact that an individual could be identified from that information. This means that data items such as name, address, date of birth, telephone numbers and even images should be handled appropriately. In isolation, some of these items may not be of concern and would not necessarily identify an individual. However, there is a risk that an amalgamation of several data items may identify an individual and therefore could lead to inappropriate disclosure of personal details. The following link provides a useful test to check that the information you hold 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

It follows that data containing personal information needs to be treated with care. The Data Protection Act 1998 contains 8 enforceable principles of good practice which should be adhered to at all times when using, storing, accessing and sharing personal information: Personal information must 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

If personal details are not kept secure, it may lead to that individual becoming exposed to risks such as fraud, theft and even their personal safety could be compromised.

For further information about the rules around Data Protection, please refer to Rotherham Borough Council's Data Protection Policy: (particularly section 7.7)

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, ensure that you have the permission of a member of staff or an administrator. Devices such as digital cameras, USB memory sticks, CD's/DVD's, mobile phones, MP3 players and even personal laptops may contain viruses that could be a potential threat to a computer or network.

If you are working with data and images of other individuals, care must be taken not to save onto any removable device without either the permission of the individual/s or a member of staff. If the device is stolen or misplaced, personal information may be disclosed and this would constitute a security breach which will be investigated.

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

BECTA - "Good practice in information handling" guide:
http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_saf_se_03&rid=14734

Internet

Both this policy and the AUP poster (for all staff, Governors, visitors and children and young people) are inclusive of both fixed and mobile internet technologies which includes Desktop PC's, laptops, notebooks, netbooks, personal digital assistants (PDAs), tablets, webcams, interactive whiteboards, voting systems, digital video equipment and technologies owned by children, young people and staff such as laptops, mobile phones, digital cameras, PDAs and portable media players, etc.

The Internet is an open communication medium, available to most people, 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 or vulnerable people.

These risks may include:

- Commercial issues with spam and other inappropriate email.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- Online content which is abusive, harmful (pro-suicide, eating disorders, etc.), pornographic, or otherwise illegal (such as promoting terrorism, gangs or weapons).

All users of the Internet should follow these basic principles of good practice guidelines and in line with other established policies:

- 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 and appropriate action taken.

- The school or other educational setting maintains that students will have supervised access to Internet resources (where reasonable) through fixed and mobile internet technology.

- Staff should review any recommended Internet sites before use in addition to those that are currently disallowed through existing filtering software.

- 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 from other sources.

- All users must observe copyright of materials including text and images.

- Schools and other educational settings should be aware of its responsibilities when monitoring communication under current legislation such as the Data Protection Act 1998, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998. The School or other educational setting will not monitor staff except in specific situations where misconduct or misuse is suspected, but it should be noted some systems designed to monitor the safety of students may not be able to discriminate between staff and student logons.

- If staff or children and young people discover an unsuitable site, the incident should be reported immediately to an appropriate member of staff.

- It is the responsibility of the school or other educational setting 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 a member of staff or Network Manager.

- If there are any issues related to viruses or anti-virus software, a member of staff or the Network Manager should be informed.

Currently the Internet technologies children and young people are using both inside and outside of the learning environment include:

- Websites
- Learning Platforms and Virtual Learning Environments (VLE's)
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs, Wikis and tweets
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functions
- Other mobile devices with web functionality

Whilst the Internet can be both beneficial and exciting in and out of a learning context, it is not consistently policed largely due to the fact that it is impossible to do so. All users need to be aware of the range of risks associated with the use of Internet technologies.

It is also important that staff and other adults are clear about procedures, for example; only contacting children and young people about homework via a school email address or school telephones, not personal email addresses or mobile phone numbers, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst a school or other educational setting acknowledges that they will endeavour to safeguard against all risks, they may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people are protected.

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 Smartphones are familiar to children outside of an educational setting too. They often provide a collaborative, well known medium with possible Internet access but equally, they expose risk and misuse associated with communication and Internet use.

Emerging technologies should be examined for educational benefit and the risk assessed before use is allowed.

Schools and other educational settings should manage the use of these devices in the following ways so that users exploit them correctly and appropriately:

- Staff and other adults are allowed personal mobile phones and other devices for their own use. Under no circumstances should a member of staff contact a pupil or parent using their personal phone.

- Children and young people are allowed to bring in personal mobile devices/phones but must not use them for personal purposes within school time or when advised by the individual establishment. At all times, the device must be switched off. There should be no reason for children and young people to require access to such devices particularly whilst in a school environment.

- The school or other educational setting 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 (within or outside an educational setting) is not allowed and may result in a serious offence being committed.

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

- Where the educational setting provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

- Where the educational setting provides a laptop for staff or other adults, only this device may be used to conduct educational business outside of the educational setting.

Social Networking / Web 2.0

Social networking sites or Web 2.0 technologies, if used responsibly both outside and within an educational context can provide easy to use, creative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, staff, other adults, children and young people should think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

One of the key benefits of social networking sites is that they encourage children and young people and adults to be creative users of the Internet. They can express themselves with an online personality, use all the applications the site has to offer, chat and socialise with peers, and share multimedia content such as music, photos and video clips with others.

There are concerns that staff, other adults and children and young people may upload content that is inappropriate, offensive or even illegal to their online spaces, posting material that could damage their reputations or the reputations of others. Equally they may post inappropriate comments to the profiles of others, which can result in bullying, slander or humiliation of others.

Many adults and children and young people maintain very detailed online profiles, including a large amount of personal information, photos and accounts of daily routines which could lead to them being identified or contacted in person. The contact risks of other forms of new technology are well documented, and those that seek to harm or exploit children and young people will use social networking sites as another way to contact and groom potential victims. Most social networking sites do contain privacy settings, allowing a profile to be set to private and only viewed by approved contacts, but these are not always used. Indeed, one of the big attractions of social networking sites is the large numbers of ‘virtual’ friends that can be linked from a profile, but this can expose adults and children and young people to the risks of unwelcome contact.

Staff may also put themselves at risk of cyberbullying by placing too much personal information on social networking sites that can be used against them by disaffected children, young people or family members.

At present, access is denied to social networking sites to staff and children and young people within an educational setting 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.)

The following advice and good practice guidance should be followed in order to stay safe whilst using social networking sites:

- All staff, other adults, children and young people are advised to be cautious about the information given by others on sites. For example; users not being who they say they are.

- Users should avoid placing images of themselves, family, friends or colleagues or details (metadata) within images that could reveal background

information on such sites and to consider the appropriateness of any images posted due to the difficulty of removing an image once posted online.

- Users should avoid giving out personal details on such sites which may identify them and their whereabouts (full name, address, mobile/home phone numbers, school details, email address, specific hobbies/interests, etc.).

- 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.

- Report any incidents of bullying (including cyberbullying) to an appropriate member of staff including any material or instructions you are uncomfortable with.

- Staff and other adults must never use social networking sites to contact children and young people outside of an educational environment even when considering replying to a message or invitation. The intention may be completely innocent, but this would be very difficult to prove in the event of the action being reported.

- Children and young people must never use social networking sites to contact staff or other adults in an educational setting using personal profiles whilst in a private or home environment. Communication should be made within an educational networking environment (For example, homework messages). Social networking sites of any kind should never be used to embarrass, upset or bully staff, other adults or children and young people.

- All users' must abide by the terms and conditions of social networking sites and must never create false profiles including age.

For further advice and guidance about social networking:
http://www.ico.gov.uk/youth.aspx
http://www.yhgfl.net/eSafety/Safer-Internet-Day-2010

Images

Digital images are easy to capture, reproduce and publish and, therefore, easy to misuse. We must remember that it is not always appropriate to take or store images of any member of the educational community or public, without first seeking permission and considering the appropriateness or consequences. An image that identifies a living individual or individuals is regarded as personal data as defined by the Data Protection Act 1998 in the same way that written data is. It is important that the following statements are adhered to:

- With the written consent of parents, (on behalf of children and young people) appropriate capture of images by staff and other children and young people is permitted. Generally, in an educational setting, permission or consent is collected at the beginning of a new academic year particularly with any new starters and those joining throughout all year groups. Consent forms can be

included in an induction or welcome pack for example and lasts for the period of time the child / young person is at the establishment (see below).

- Staff, children and young people are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of children and young people or staff. This includes when on field or residential trips. However, with the express permission of the Head teacher or other suitable member of staff, images can be taken provided they are transferred immediately and solely to the network and deleted from the device. There are exceptions to these rules; children and young people may wish to capture and keep images for personal use and this is permitted providing that the subject/s is/are aware and has given permission to be filmed or photographed. A Head teacher or supervisor may use their discretion as to whether mobile phones or cameras are permitted on trips at all and the decision should be documented. It follows that is advisable for educational establishments to create a policy (or provide a statement on a consent form) clearly stating the rules around use of images.

- In certain cases, images stored on a network, may be open to tampering in a negative way.

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

Consent of staff and other 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 retained on their personnel file.

Publishing children and young people's images and work

Parents will be given the opportunity to grant permission (via a consent form) to enable their child's work/photos to be used in the following ways:

- on a website
- on a Learning Platform / VLE
- 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 or young person attends a school or other setting unless there is a change in circumstances. Parents may withdraw permission, in writing, at any time.

Children and young people's 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.

Schools and other educational settings should be mindful not upload students work that may be copyright e.g. music, photographs, etc.

School website (if different to the Learning Platform / VLE space)

The uploading of images to an educational website will be subject to the same acceptable rules as uploading to any personal online space. Permission should always be sought from the parent prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

Webcams, video conferencing and CCTV

- A school or other educational setting should use Closed Circuit Television (CCTV) for security and safety appropriately and according to data protection principles. (Rotherham MBC CCTV Policy and Guidance): https://public.rgfl.org/esafety/Information%20Governance/CCTV%20Policy%20and%20Guidance%202009-10%20.doc

- Webcams should only ever be 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 web cams are used, consent should be sought from parents and staff in the same way as for all other images.

Video hosting sites

Images and video can be posted to blogs and social networking sites and sent by email and mobile phone. There has been a tremendous rise in the popularity of video hosting sites, such as YouTube, where clips are uploaded and shared. Popular video clips can be seen by hundreds of thousands of visitors to the sites, and clips are rated by viewers, and comments (including video comments) can be posted about them. The video footage can also be embedded in other sites and pages.

There can be a lot of useful content to view on these sites; music videos, amusing clips and other entertainment, as well as useful resources, including educational resources. Even Internet safety and anti-bullying videos can be found on these sites. Video is stored on and streamed from the sites themselves, which means that viewing is very easy.

There are two ways that children and young people may be exposed to risk on video hosting sites: accessing inappropriate material (e.g. violent, pornographic or illegal content) and they may post inappropriate material, which might make them contactable and vulnerable or which might lead to embarrassment for themselves or others.

Video hosting sites can be misused for cyberbullying, and staff as well as children and young people have been victim to content posted upon such sites. Cyber bullying may take the form of video taken without the subject's knowledge, even from within an educational environment that is then posted and shared.

- Under no circumstances should images, sound or text be used to cause embarrassment, upset or used to threaten anyone both in an educational setting

or private environment as this may lead to sanctions placed upon the individuals and may possibly lead onto criminal prosecution.

Behaviour and respect (Behaviour and Anti Bullying Policies)

Refer to the Behaviour Policy (including anti bullying) for procedures in dealing with any potential bullying incidents via any online or offline communication, such as mobile phones, email or blogs.

All behaviours should be regarded as and dealt with in exactly the same way, whether online or offline and this needs to be a key message which sits within the ICT and PSHE curriculum for children and young people and their parents. People should not treat online behaviours any differently to offline behaviours and they should have exactly the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies. It is only the tools and technology that change, not the behaviour of children, young people and adults.

Allegation procedures involving staff and other adults

Please refer to the Child Protection Policy where applicable or the eSafety incident flowchart (see Appendix D) in order to deal with any incidents that occur as a result of using personal mobile or email technologies which may result in an allegation of misuse or misconduct being made by any members of staff or children and young people about a member of staff.

- Allegations should be reported to the Head teacher, manager or other member of staff immediately as appropriate or to the Chair of Governors in the event of the allegation made about the Head teacher.

- Personal equipment belonging to staff and other adults should not be used when contacting children and young people about homework or any other school issues either in or beyond an educational setting and any such action should be dealt with immediately.

- We follow this guidance to protect staff members from potential allegations of misconduct by a child, young person or parent.

External websites

In the event that a member of staff finds themselves or another adult on an external website of any type as a victim, they are encouraged to report incidents to the Head teacher and unions, using appropriate internal reporting procedures.

Disciplinary procedure for all education based staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online and offline technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the AUP in line with any staff code of conduct.

Complaints relating to staff and children and young people

- Complaints relating to acceptable use should be made to an eSafety coordinator, Head teacher or Line Manager/Supervisor where appropriate. Incidents should be logged (see Appendix E) and the flowchart for managing incidents should be followed (see Appendix D).

- For less serious incidents*, it may not be necessary to take any action by using the eSafety incident flowchart. If you witness, or are informed of anyone acting inappropriately, you should politely remind them of the AUP and any other rules depending on the circumstances and environment.

- If you do not want to approach the user or are unsure of the seriousness of the incident, or the incident has been reported after the user has left, you should report the incident to a senior member of staff who will progress the matter as appropriate and where necessary.

- Where children and young people have breached the conditions of the AUP, any misuse may be reported to the parent depending upon the seriousness of the incident.

*Less serious incidents may be: a user being heavy handed with ICT equipment; volume of equipment too loud; disruptive or loud behaviour; Spilled food or liquid damaging equipment.

Section 7 Managing an eSafety incident

Reporting

All eSafety incidents should be reported to the eSafety coordinator[2] or appropriate member of staff, who will log them and decide on appropriate action. This may include involvement of senior staff and leaders within the educational setting. External agencies, such as the Rotherham Safeguarding Children Board (RSCB), the Police or another appropriate agency, may also need to be notified.

Managing your response

No two eSafety incidents will be exactly the same and should therefore be dealt with and judged on their own merits. Different eSafety incidents will require different approaches.

In managing the response, this AUP should be referred to as it clearly defines what is 'inappropriate' in various eSafety scenarios, and the sanctions that will apply.

Refer to the Appendices at D and E to assist with the decision and record making process when responding to all incidents.

[2] Secondary schools are encouraged to have a designated eSafety Coordinator whilst in primary schools; the eSafety coordinator can be the Child Protection Officer.

Section 8 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 children and young people, and how these might affect their approaches to learning:

- Special Educational Needs (e.g. Asperger Syndrome, Dyslexia, Dyspraxia, Attention Deficit Hyperactive Disorder (ADHD), general learning difficulties, etc.)
- Difficulties with communication, language and literacy
- Behavioral difficulties
- Physical impairment
- Emotional difficulties
- English as an additional language (EAL)
- Race and ethnicity
- Religious belief
- Gender issues
- Social background
- Ability
- Looked After Children and Children In Need

Children with special educational needs or particular vulnerability

The Staying Safe Action Plan identifies that targeted safeguarding is needed for some groups of children who are at greater risk than others, and it is important to target policies and services to these groups to help keep them safe from harm. This might include children and young people with special educational needs, mobile or travelling children, children for whom English is an additional language, those in hospital, residential, or special schools, children in pupil referral units, or those receiving social care. Children in these groups may be particularly vulnerable to eSafety risks. Below are some examples:

• **Levels of understanding**: degrees of general learning difficulty (and how these interact with maturity) will determine how far children are aware of social and other implications of the content of their communication – both in expression and in making sense of communication received. There may be a discrepancy between both the maturity and the learning difficulties of the sender of messages and the recipient, and vice versa. Certain forms of special need, such as autism, may result in children making particularly literal interpretations of content, which will affect the sense they make of communications.

• **Understanding of technology**: vulnerable children and young people may also misjudge communication and be unaware of how widely messages may be disseminated. They may also have difficulty in appreciating the need to restrict access to personal information or use of personal videos, for example.

• **Language barriers**: those new to English may not be familiar with the social implications in the use of language, and the same may apply to their parents.

• **Physical or sensory disabilities**: children and young people with physical or sensory disabilities may be attracted by the anonymity of communication, and the scope for incognito presentations of themselves. The 'unreality' to which this gives rise may have unfortunate consequences.

• **Emotional and behavioural difficulties**: children with emotional and behavioural difficulties may well express these in their communications and may not allow for the effect this may have on the recipients – and on the response their communication evokes. This may lead to heightened emotional involvement with unrealistic expectations as a consequence.

• **Settings**: children in restricted settings with high levels of supervision are likely to be protected from some of the more obvious risks. Consequently, they may not be aware of risks in using technology in non restricted settings such as their own homes, internet cafes or libraries and may not be well equipped to respond to these.

• **Supervision**: those responsible for supervision in settings must be aware of the very real dilemma they face in balancing their concern to protect children from risk with their obligation to recognise children's rights to express themselves and interact with their peers and others. This particularly applies as children get older. In particular, difficulties may arise in relation to learners being advised not to disclose their passwords but needing assistance to use, or remember them, and the need to exercise a duty of care. Those responsible for delivering services to children with special educational needs or particular vulnerabilities are best placed to understand the unique characteristics of those in their care, and should carefully consider their specific needs with regard to eSafety.

Equal opportunities and inclusive practice in an educational setting involves careful planning by all professionals concerned to ensure effective learning opportunities for all children and young people.

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

Section 9 Writing and reviewing this policy

Individual involvement in policy creation

Staff, children, young people and parents should be actively encouraged to review this policy through staff meetings, School Council or Youth Clubs for example. Ownership of all those involved will help to encourage and empower users of ICT to accept the guidance and sanctions laid down in this policy.

Review procedure

This policy will be reviewed every 12 months and consideration given to any comments or suggestions received for future versions. It is anticipated that any new version will be made available and educational settings informed when the time arises.

The policy will also be amended to reflect when new technologies are adopted or Central Government change any orders or guidance in any way.

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/Supervisor.
- I will not install any hardware of 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/Supervisor.
- 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/Supervisor.
- 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 the above statements and to support the safe use of ICT

Signature …… Date ……

Full Name …….... (Please print)

Job title ……

ICT Rules

We always ask permission before using ICT equipment

We learn to keep our passwords a secret

We only ever log onto a computer as ourselves

We never give out our names, phone numbers or home address to anyone

We never arrange to meet someone we don't know – ask an adult we know and trust first

We only use websites that an adult has chosen or knows about

We can write polite and friendly emails to people that we know

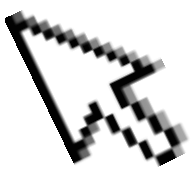
We close any website that we don't like and tell an adult

We never open emails from anyone who we don't know

We know who to ask for help if we are not sure about anything

We know that it is important to follow these rules to keep us safe and to treat ICT equipment with care.

Think b4 u click!



School/setting logo and details

Dear Parent/Carer

ICT including the Internet, Learning Platforms, email and mobile technologies have become an important part of learning. We expect all children and young people to be safe and responsible when using ICT. It is essential that children and young people are aware of eSafety and know how to stay safe when using ICT both within learning and home environments.

Your child is expected to read and discuss this agreement with you and then to sign and follow the terms of the agreement. Any concerns or an explanation can be discussed with [*name and contact details*]

Please return the bottom section of this form to [*name and address of establishment*].

✂ -

ICT Acceptable Use Policy (end user agreement for Key Stage 1 & 2)

Pupil and parents agreement

We have discussed this document and *……………………………. agrees to follow the acceptable use policy conditions above and supports the safe and responsible use of ICT.

*Child's full name in block capitals

Parents signature: …….…………………….…………………………...............

Childs signature: ……………………………………………………………….

Form**: ………………………………………………………………………………

Date: ………………………………

**Or name of establishment if not school

Appendix **B** (Design 2)

ict rules

We always ask permission before using the ICT equipment.

We learn to keep our passwords a secret.

We only ever log onto a computer as ourselves.

We never give out our names, phone numbers or home address to anyone.

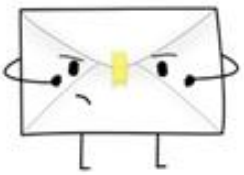
We never arrange to meet someone we don't know - ask an adult we know and trust first.

We only use websites that an adult has chosen or knows about.

We can write polite and friendly emails to people we know.

We close any website we don't like and tell an adult.

We never open emails from anyone we don't know.



We know who to ask for help if we're not sure about anything.

We know it's important to follow these ICT rules to keep us safe and to treat equipment with care

'Think b4 u click'

School/setting logo and details

Dear Parent/Carer

ICT including the Internet, Learning Platforms, email and mobile technologies have become an important part of learning. We expect all children and young people to be safe and responsible when using ICT. It is essential that children and young people are aware of eSafety and know how to stay safe when using ICT both within learning and home environments.

Your child is expected to read and discuss this agreement with you and then to sign and follow the terms of the agreement. Any concerns or an explanation can be discussed with [*name and contact details*]

Please return the bottom section of this form to [*name and address of establishment*].

✂ -

ICT Acceptable Use Policy (end user agreement for Key Stage 1 & 2)

Pupil and parents agreement

We have discussed this document and *……………………………. agrees to follow the acceptable use policy conditions above and supports the safe and responsible use of ICT.

*Child's full name in block capitals

Parents signature: …….……………………….………………………..............

Childs signature: ……………………………………………………………….

Form**: ……………………………………………………………………………

Date: ………………………………

**Or name of establishment if not school

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.

Passwords 	• I will only use my own ID and password to log onto a computer. • I will not give out my password to anyone. • I will log off properly after I have finished with the computer.
Email 	• I will not access or create any material that may cause upset to others. • If I am unsure about opening or downloading any attachments or contents of an email, I will ask a member of staff. • I will not send abusive or threatening language in an email to others.
Data Security 	• I will keep my personal information safe from other people. • I will not access any other user's files and folders without permission. • I will not use portable media (like memory sticks) on the network without asking a member of staff first.
Internet 	• I will not browse or download anything illegal and forward or share any material that could cause upset to anyone. • If I do come across any such material I will report it immediately to a member of staff. • I will not attempt to bypass the internet filtering system. • I will not attempt to access any unsupervised/unauthorised chatrooms or areas.
Images 	• I will only take, store and use images of children, young people and/or staff for an agreed project or purpose. • I will only use images outside the network if I have permission from the people in the image and a member of staff. • I will only use images that have been approved by a member of staff.
Behaviour 	• I will only communicate with others online sensibly. • I will not send or encourage others to send abusive messages. • I will make sure that any online or offline activity will not cause the school/centre, staff and any other user, distress or embarrassment.
	• I know that all use of the network is monitored if abuse is suspected. • I will treat other people and ICT equipment with care and respect. • 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.

School/setting logo and details

Dear Parent/Carer

ICT including the Internet, Learning Platforms, email and mobile technologies have become an important part of learning. We expect all children and young people to be safe and responsible when using ICT. It is essential that children and young people are aware of eSafety and know how to stay safe when using ICT both within learning and home environments.

Your child is expected to read and discuss this agreement with you and then to sign and follow the terms of the agreement. Any concerns or an explanation can be discussed with [*name and contact details*]

Please return the bottom section of this form to [*name and address of establishment*].

✂- -

ICT Acceptable Use Policy (end user agreement for Key Stage 3 & 4)

Pupil and parents agreement

We have discussed this document and *……………………………. agrees to follow the acceptable use policy conditions above and supports the safe and responsible use of ICT.

*Child's full name in block capitals

Parents signature: …….……………………..……………………………..............

Childs signature: ……………………………………………………………….

Form**: ………………………………………………………………………………

Date: ………………………………

**Or name of establishment if not school

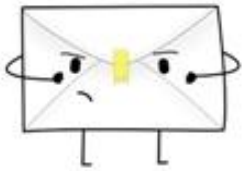
ICT RULES

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.

**** • Passwords

I will only use my own ID and password to log onto a computer.
I will not give out my password to anyone.
I will log off properly after I have finished with the computer.



• E-mail

I will not access or create any material that may cause upset to others.
If I am unsure about opening or downloading any attachments or contents of an email, I will ask a member of staff.
I will not send abusive or threatening language in an email to others.

• Data security

I will keep my personal information safe from other people.
I will not access any other user's files and folders without permission.
I will not use portable media (like memory sticks) on the network without asking a member of staff first.

• Internet

I will not browse or download anything illegal and forward or share any material that could cause upset to anyone.
If I do come across any such material I will report it immediately to a member of staff.
I will not attempt to bypass the internet filtering system.
I will not attempt to access any unsupervised/unauthorised chatrooms or areas.

• Images

I will only take, store and use images of children, young people and/or staff for an agreed project or purpose.
I will only use images outside the network if I have permission from the people in the image and a member of staff.
I will only use images approved by a member of staff.

• Behaviour

I will only communicate with others online sensibly.
I will not send or encourage others to send abusive messages.
I will make sure that any online or offline activity will not cause the school/centre, staff and any other user, distress or embarrassment.

• Respect

I know that all use of the internet is monitored if abuse is suspected.
I will treat other people and ICT equipment with care and respect.
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.

School/setting logo and details

Dear Parent/Carer

ICT including the Internet, Learning Platforms, email and mobile technologies have become an important part of learning. We expect all children and young people to be safe and responsible when using ICT. It is essential that children and young people are aware of eSafety and know how to stay safe when using ICT both within learning and home environments.

Your child is expected to read and discuss this agreement with you and then to sign and follow the terms of the agreement. Any concerns or an explanation can be discussed with [*name and contact details*]

Please return the bottom section of this form to [*name and address of establishment*].

✂---

ICT Acceptable Use Policy (end user agreement for Key Stage 3 & 4)

Pupil and parents agreement

We have discussed this document and *……………………………. agrees to follow the acceptable use policy conditions above and supports the safe and responsible use of ICT.

*Child's full name in block capitals

Parents signature: …….…………………….…………………………...............

Childs signature: ……………………………………………………………….

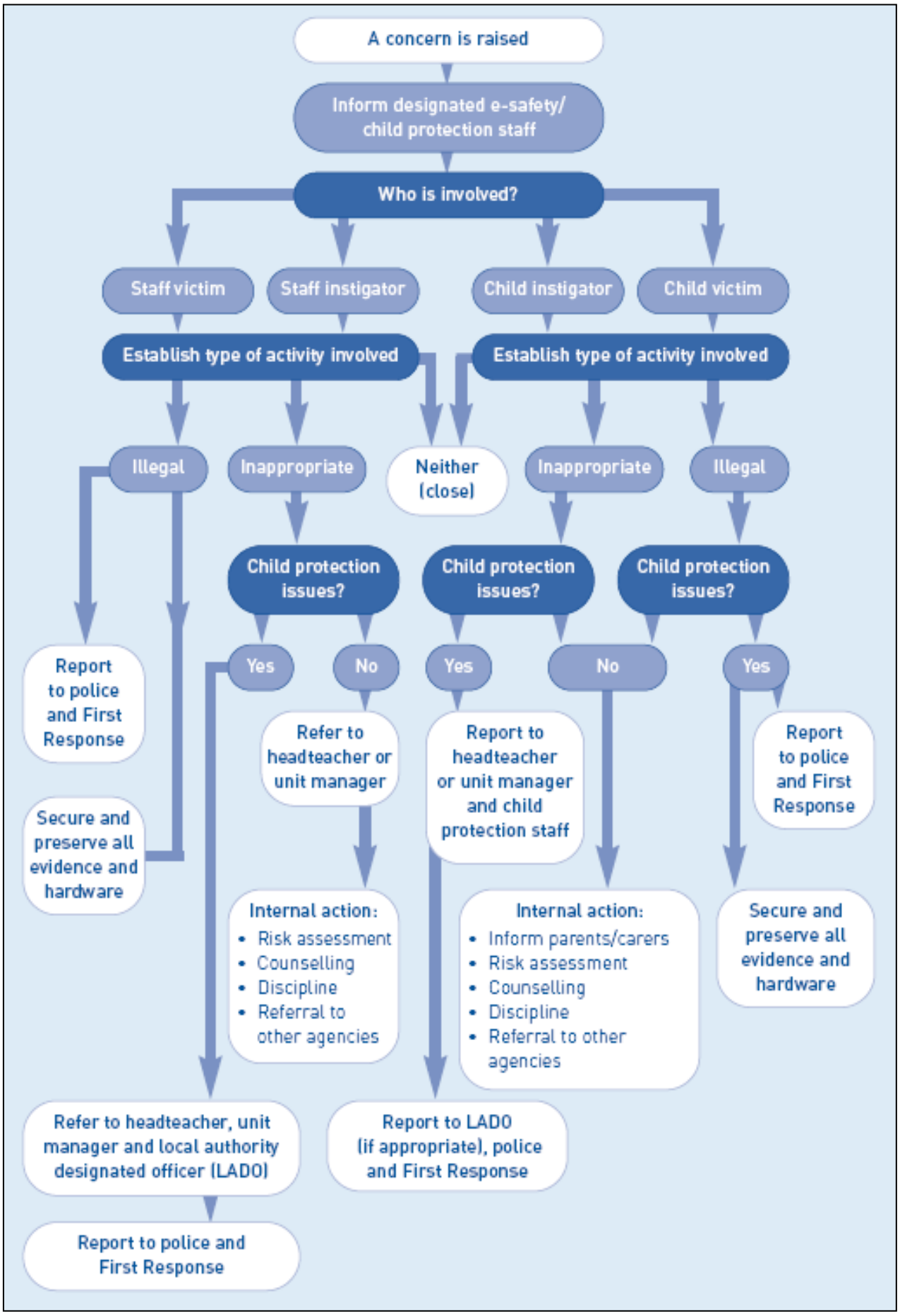
Form**: ………………………………………………………………………………

Date: ………………………………

**Or name of establishment if not school

Appendix **D**

Flowchart for managing an eSafety incident



(Courtesy of Staffordshire County Council)

Appendix **E**

eSafety 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	

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.hmso.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.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
The Act is one of the most significant pieces of constitutional legislation enacted in the United Kingdom. It is a key part of the Government's programme to encourage a modern civic society where the rights and responsibilities of our citizens are clearly recognised and properly balanced. Its effect is to allow people to claim their rights under the European Convention on Human Rights in UK courts and tribunals, instead of having to go to the European Court in Strasbourg. The Act underpins this by requiring all public authorities in the UK to act compatibly with the Convention rights. This places new responsibilities on all of us who work in public authorities, which includes central government, the courts, the Police, local government and many bodies who carry out functions which the Government would otherwise have to undertake.
http://www.justice.gov.uk/guidance/humanrights.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.
http://www.opsi.gov.uk/acts/acts2006/ukpga_20060001_en_1

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.

http://www.opsi.gov.uk/acts/acts1986/pdf/ukpga_19860064_en.pdf

Crime and Disorder Act 1998

The Crime and Disorder Act 1998 promotes the practice of partnership working to reduce crime and disorder and places a statutory duty on Police and Local Authorities to develop and implement a strategy to tackle problems in their area. In doing so, the responsible authorities are required to work in partnership with a range of other local public, private, community and voluntary groups and with the community itself.

The Acts key areas were the introduction of Anti-Social Behaviour Orders (ASBO's), Sex Offender Orders, Parenting Orders and the introduction of law specific to 'racially aggravated' offences.

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.

http://www.opsi.gov.uk/acts/acts2003/ukpga_20030042_en_1

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.

http://www.opsi.gov.uk/ACTS/acts2003/ukpga_20030021_en_13#pt2-ch1-pb20-l1g127

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 persons 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.

http://www.opsi.gov.uk/acts/acts1990/ukpga_19900018_en_1#pb1-l1g1

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send a letter (including an 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.

http://www.opsi.gov.uk/ACTS/acts1988/Ukpga_19880027_en_1.htm

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.
http://www.copyrightservice.co.uk/copyright/p01_uk_copyright_law

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.
http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1978/cukpga_19780037_en_1

Obscene Publications Act 1959 and 1964
An Act to amend the law relating to the publication of obscene matter; to provide for the protection of literature; and to strengthen the law concerning pornography.
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&parentActiveTextDocId=1128038&ActiveTextDocId=1128040&filesize=45334

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.
http://www.opsi.gov.uk/acts/acts1997/ukpga_19970040_en_1

Privacy and Electronic Communications (EC Directive) Regulations 2003 (Including spam)
The Privacy and Electronic Communications Regulations set out rules for people who wish to send you electronic direct marketing, for example, email and text messages.
http://www.ico.gov.uk/what_we_cover/privacy_and_electronic_communications/the_basics.aspx

Appendix **G**

Glossary

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

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 eSecurity and eSafety 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.

eLearning: 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.

End user: The individual using ICT equipment at the time.

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

eSafety: 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.

RGfL: Acronym for Rotherham Grid for Learning - provides fast, secure and effective broadband Internet and email access for Rotherham schools. At its heart is a network

which also connects all the borough's schools together via a central point where both pupils and teaching staff can share resources.

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 eSafety and technology is evolving rapidly. You may wish to keep up to date with further information or advice which can be found from the following websites:

- www.parentscentre.gov.uk (Resource for parents)
- http://www.ceop.gov.uk/ (Child Exploitation and Online Protection Centre -Resources for schools, parents, children and young people and practitioners)
- www.iwf.org.uk (Internet Watch Foundation - reporting of illegal images or content)
- www.thinkuknow.co.uk (The Internet safety programme delivered by CEOP)
- www.netsmartzkids.org (Suitable for 5 – 17 year olds)
- http://www.kidzsmart.co.uk/index.html – (Suitable for all under children under 11 years)
- www.phonebrain.org.uk (Suitable for Years 5 – 8 year olds)
- www.bbc.co.uk/cbbc/help/safesurfing (Suitable for Years 3 and 4)
- www.hectorsworld.com (Suitable for Foundation Stage, Years 1 and 2 and is linked to the thinkuknow website above)
- www.teachernet.gov.uk (Resource for schools, LA's and other educational settings)
- www.digizen.org.uk (Materials from DfE around the issue of cyberbullying)
- www.becta.org.uk (Resource for the education sector and others including current model policies on eSafety)
- http://www.nextgenerationlearning.org.uk/ (Simple tips for parents / adults)
- http://www.rscb.org.uk/Home.aspx (Rotherham Safeguarding Children's Board – policies, procedures and practices.)
- http://www.nen.gov.uk/esafety (Resources for schools and other educational settings – including an online eSafety tool.)
- http://www.yhgfl.net/ (Yorkshire and Humber Grid for Learning – Consisting of a Regional Broadband Consortium)
- 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.)
- http://clickcleverclicksafe.direct.gov.uk/index.html (The UK Council for Child Internet Safety (UKCCIS) has launched a useful 'Click Clever, Click Safe Code designed to act as an everyday reminder of simple good behaviours, to help avoid common risks online)