St Matthew's RC High School

e-Safety Policy

Reviewed: March 2017

To be reviewed: July 2019

e-Safety Policy: St. Matthew's R.C. High School

The acceptable use of the school network, Internet and related technologies

Contents

This e-Safety Policy has been written by St. Matthew's R.C. High School.

The policy reflects the work of Holy Family RC/CofE College, Heywood, and builds on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the Senior Leadership Team and approved by Governors.

Created by: :……

Date: ……

To be revised::……

Approved: ……

Context

St Matthew's RC High School is dedicated to promoting a distinctive Catholic ethos by upholding the teachings of the Catholic Church. This means that everything we aim to achieve will be based on the teachings and practice of the Catholic Church. Our motto is "Quaerite primum regnum dei" - "Seek first the Kingdom of God" - and our aim is to achieve this motto in our school life. We will work to build God's Kingdom and be happy together because we believe that Jesus died and rose again for us and that He is always present in our school and in our world. We are committed to developing the full potential of every individual, regardless of culture, race, religion, disability, or special need by creating a safe, orderly environment where all members of the community work diligently in a spirit of co-operation and treat each other with courtesy and respect at all times.

Our primary role is to educate children and we uphold the principle outlined in the Bishop's Conference of England and Wales (2000) that:

"Education is holy … the process of teaching and learning is a holy act"

Within this context we endeavour to ensure that our pupils have access to the highest quality teaching and learning materials and experiences, involving greater use of modern technologies.

Harnessing Technology: Transforming learning and children's services[1] sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, e-Strategy 2005

It is the duty of **St Matthew's RC High School** to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the pupils, the staff, governors and the school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging
- Blogs (an on-line interactive diary)

[1] https://www.education.gov.uk/publications/standard/publicationDetail/Page1/DFES-1437-2005

- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites including video broadcasting sites
- Gaming Sites
- Music download sites
- Smart phones with camera, video, e-mail and web functionality.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

2. Teaching and Learning

2.1 Internet use will enhance and extend learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and pupils.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2 Pupils will be taught how to evaluate Internet content

- St. Matthew's R.C. High School will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Roles and Responsibilities

e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to members of the Senior Leadership Team who may also have responsibility for Child Protection.

Our school **e-Safety Co-ordinators** are **Mrs A. Ager [Deputy Headteacher], Mr P. Aulton [Asst.Head] and Miss H. Nicholls [Asst. Head],**

Our e-Safety Co-ordinators ensure they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and The Child Exploitation and Online Protection (CEOP)[2]. The school's e-Safety coordinators ensure the Headteacher; Senior Leadership Team and Governors are updated as necessary.

[2] http://www.ceop.gov.uk/

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a culture where pupils feel able to report any bullying, abuse or inappropriate materials. Staff are expected to complete an e-learning courses on 'online safety'.

All staff should be familiar with the school's policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- Anti-bullying procedures;
- their role in providing e-Safety education for pupils;
- acceptable use of school social media accounts;

The school's ICT service, in liaison with senior staff will be responsible for the blocking of email, internet and network access following an infringement. They will liaise with the e-Safety Co-ordinators will liaise with the school's ICT service to investigate the infringement and the imposition of agreed sanctions.

Staff are reminded/updated about e-Safety matters at least once a year via Inset training in September.

3.1 Safe use of email.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher or other member of staff if they receive offensive e-mail.
- In e-mail communication, pupils should not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school's ICT service will block the receipt of email to pupils on the network from external sources and will stop the forwarding of chain letters.

3.2 Safe use of Internet including use of internet-based communication services, such as instant messaging and social network.

- The school's ICT service will block access to social networking sites except at designated times.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. This is reinforced through work in VT and ICT curriculum activities.

3.3 Safe use of school network.

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school network uses two main filtering systems, 'smoothwall' blocks access to websites deemed unsuitable. This list is regularly reviewed and new sites added as appropriate.
  Esafe is an active monitoring system, that looks at the key strokes by all users and if there is concern this is reported to school for further action. Each report is reviewed by A Ager and the appropriate action is taken.
- If staff or pupils discover an unsuitable site, they should contact school's ICT service immediately so the address can be blocked and should the report to the e-Safety co-ordinators.
- All users are asked to respect the privacy of files of other users. Pupils are asked not to enter file areas of other users without obtaining permission first. All users are reminded that files to be shared should be saved to the shared areas available
- All users accessing software or any services available through the school network must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. All users should be aware that some items are licensed for educational or restricted use only.

3.4 Safe use of passwords.

- All users are expected to be responsible for their own areas on the school network.
- Passwords are set for each user.
- Passwords should be a minimum of 8 characters and recommended to be a mix of letters (upper and lower case), numbers and characters.
- Passwords should not be shared with other users.
- It is recommended that passwords are changed regularly.

3.5 Safe use of equipment.

- Pupils must treat with respect equipment in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers.
- Pupils should be reminded that any malicious action will result in the immediate suspension from use of the school facilities.

3.6 Protection of personal data.

- Personal data will be recorded, processed, transferred and made available according to the current data protection guidelines.

3.7 Publication of pupil information, photographs and use of website.

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified by name.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- At the admission interview for pupils, parents/carers are informed that photographs including images of pupils will be used on display boards, the school website and other promotional materials for the benefit of the school. Parents/ carers sign a form to give their permission for photographs of their child to be taken at the admission interview.
- Staff or pupil personal contact information will not be published i.e. addresses and personal telephone numbers. The contact details given online would normally be via the school office.
- The Headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

3.8 Safe use of digital images and digital technologies, such as mobile phones and digital cameras.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- All staff should note that technologies such as mobile phones with 3/4G capability will bypass school filtering systems and present a new route to undesirable material and communications.
- Pupils who choose to bring mobile phones into school do so at their own risk. St. Matthew's R.C. High School does not take any responsibility for them. Pupils using mobile phones in school to phone or text after 8.30am except for break and lunch will have them confiscated and only returned to a parent/carer.
- The use by pupils of digital cameras, mobile phones containing digital cameras is not permitted. Pupils may only access digital cameras via curriculum based activities and under the supervision of staff
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. They are only to be used under direct supervision.
- Staff will be issued with a school phone where contact with pupils is required.

3.9 e-Bullying and Cyber bullying procedures.

- Cyber bullying can be defined as abusive or threatening behaviour via text messaging, e-mail, chat rooms, discussion boards, social networking sites and instant messaging services.
- Pupils must be made aware that this behaviour will not be tolerated and also that sending abusive or threatening messages is against the law. It is also against the law to forward abusive texts, e-mails, messages or images.
- Cyber bullying will be treated in line with St. Matthew's R.C. High School's anti-Bullying policy. Pupils who are being bullied by email, text or online should keep and save any bullying emails, text messages or images, and note times and dates of messages and details about the sender.
- Staff and pupils should refer to the Progress Leader in the first instance who may consult with designated safeguarding officers – **Mrs A. Ager [Deputy Headteacher], Mr P. Aulton [Asst. Head] and Ms H.Nicholls [Asst. Head].** The incident will then be investigated in line with the Anti-Bullying policy and if appropriate reported through established safeguarding procedures.
- Incidents involving sending photographs between pupils that might be considered sexting will be dealt with following the guidance in 'Sexting in schools and colleges' UKCISS 2016

3.10a Use of social networking sites

- In their own interests, adults within school settings need to be aware of the dangers of putting their personal information onto social networking sites, such as addresses, home or mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.
- All adults, particularly those new to the school setting, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.
- Adults should never make a 'friend' of a pupil or 'follow' a pupil at the school where on their social networking page, and should be extremely cautious about becoming 'friends' with ex-pupils particularly where siblings or other relatives may continue to attend the school.
- Staff should never use or access social networking pages of pupils.
- Confidentiality must be considered at all times. Social networking sites have the potential to discuss inappropriate information and staff need to ensure that they do not put any confidential information on their site about themselves, the school, the governing body, the Local Authority, their colleagues, pupils or members of the public.

- Staff need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other members of staff, pupils or other individuals connected with the school, or another school, or the Local Authority could result in disciplinary action being taken against them.
- Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school into disrepute or that could be interpreted as reflecting negatively on their professionalism.
- Some social networking sites and other web-based sites have fields in the user profile for job title etc. As a member of staff of the school and particularly if you are a teacher or teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school and the profession.

3.10b SMRCHS Social Media (Twitter) Acceptable Use Policy.

These are the guidelines and behaviours that users are expected to follow when interacting with any of St Matthew's RC High School's Twitter accounts. This includes interactions via 'hashtags', using the school account tags e.g. @SMRCHS, making mention of school accounts through tweets, retweets, quotes, direct messaging or making tweets a favourite.

I. School twitter accounts are intended for educational purposes and the purpose of sharing associated information
II. All activity over school twitter accounts will be monitored and retained
III. Pupils and other stakeholders are expected to use this social media responsibly and respectfully – as they would conduct themselves offline.
IV. Misuse involving school twitter accounts will result in appropriate sanctions.
V. Followers of school twitter accounts and users of twitter should alert a member of the senior leadership team of any concerns for safety or security.

3.10c Designated Staff Operation of SMRCHS Twitter Accounts

St Matthew's RC High School allows designated staff to operate Twitter accounts for the sole purpose of school-related communication for their subject area.

Any department who would like to operate a twitter account for their subject area should see A Ager or L Dooley – who centrally monitor all school twitter accounts and ensures consistency in our approach.

Staff who are provided with access to Twitter accounts, should ensure they are used with due care.

- Staff should not send personal information about themselves or any pupils;
- Staff should not attempt to open files or follow links from unknown or untrusted origins;
- Staff should use always use appropriate, professional and grammatically correct language;
- Staff should take due care when using a 'hashtag' and ensure no links to inappropriate conversation threads;
- Staff should not communicate with individual pupils / parents using twitter.
- Staff should only post pictures of pupils for whom we have photographic permissions for, and verbal permissions for from pupils. Pupil's full names must not be put on twitter. LAC must not appear on any photos.
- Staff should not follow any pupils or parents back, and should only follow appropriate, trusted educational twitter accounts.

- Staff are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline.
- Twitter posts may be monitored and archived indefinitely.

3.11 Curriculum role in providing e-safety education for pupils.
All pupils will be given e-Safety lessons during each academic year as part of the curriculum schemes of work.

4. Policy Decisions

4.1 Authorising Internet access.
- All staff must read and sign the Acceptable Users Policy (see appendix 1.1) when they start employment.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Parents/carers and pupils will be asked to sign the acceptable use policy in the journal.

4.2 Assessing risks.
St. Matthew's R.C. High School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective. This will take place on an annual basis

4.3 Handling e-Safety complaints.
- Complaints of Internet misuse will be dealt with by the e-Safety Co-ordinators.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents/guardians will be informed of the complaints procedure.
- Discussions will be held with the School Police officer to establish procedures for handling potentially illegal issues.

5. Communicating e-Safety

5.1 Introducing the e-Safety policy to Pupils.
- Pupils will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be delivered each academic year.

5.2 Staff and the e-Safety policy.
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff should understand that phone or online communications with pupils can lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

- Staff should refer to the document **"Guidance for Safe Working Practice for the Protection of Children and Staff in Education Settings" (to be found in the Staff Handbook folder on the Shared Area):** Communication with children and adults, by whatever method, should take place within professional boundaries and staff should avoid any personal subject matter. This includes the wider use of technology such as mobile 'phones, text messaging, e-mails, digital cameras, videos, web-cams, websites, social network sites and blogs.

5.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, expectations booklet and on the school web site.
- An introduction to safety is provided for parents in year 7 as part of the 'Academic evening' at the start of year 5

6. Infringements and Sanctions

Any failure to comply with the Acceptable User Policies may lead to temporary or permanent suspension of the use of ICT facilities. The Headteacher, within their discretion, may waive or vary a penalty if the circumstances warrant such action.

6.1 Pupil infringements and Sanctions

Where a pupil fails to adhere to the responsible user's agreement, sanctions will be imposed. The final level of the sanction will be at the discretion of the Senior Leadership Team via discussion with the appropriate subject leader/progress leader.

6.2 Staff infringements and Sanctions

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. during non contact time.
- The above activities must never take place in front of pupils during lesson (contact) time.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on school network.

Sanction: Referral to Line Manager. Headteacher Warning given.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to any school computer hardware or software.
- Any deliberate attempt to breach data protection or computer security rules.
- Deliberately accessing and downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988.
- Bringing the school name into disrepute, this includes the discussion of school activities, in a negative way, on social networking sites.
- Inappropriate communications with pupils and minors under the age of 18.

Sanction: Referral to Headteacher and Governors. School disciplinary procedures followed.

Other safe guarding actions:

- Removal of staff PC to a secure place to ensure that there is no further access to the PC/
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing

inappropriate materials in school.
- Identify the precise details of the materials.

St. Matthew's R.C. High School may involve external support agencies as part of the investigation of any breach of the e-safety policy e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.
In the case of Child Pornography being found, the member of staff will be immediately suspended and the Police will be called. Be aware that anyone can report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): http://ceop.police.uk/safety-centre/ or to Manchester Children's Services

6.3 Informing Staff and Pupils of procedures

- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so that they develop 'safe behaviours'.
- Staff and Pupils will be required to sign the acceptable user policy.
- Staff will be made aware of the infringements and sanctions via Inset training and the staff handbook. The e-Safety policy will be available via the staff shared area.
- Pupils will be made aware of the infringements and sanctions via curriculum and posters made available in networked areas.
- The school e-Safety policy will be made available to all users, parents/guardians via St Matthew's RC High School web site

Appendix 1

St. Matthew's R.C. High School

Responsible ICT System and Internet Use - Pupils

This responsible Internet Use statement helps to protect pupils, staff and the school by clearly stating what use of the computer resources is acceptable and what is not.

We expect all pupils to be responsible for their behaviour when using ICT and the Internet. It is essential that pupils are aware of e-Safety and know how to stay safe when using ICT.

- I will only use the school's ICT system including the Internet, email, digital video etc for school purposes, and only when under the supervision of a member of staff.
- I will only access the school network using my own user name and password and will not access other user's files.
- I will follow the school's ICT security system and not reveal my password to anyone.
- I will check with the Teacher before using any removable media such as pen drives or CDs on the computers in school.
- I will use my school email address for all email communication with other pupils and staff.
- I will ask permission from a teacher before checking any non school email accounts on the Internet, such as gmail.
- I will make sure that all ICT communications with pupils, teachers or others are responsible and polite.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download or upload material that could be considered to be offensive or illegal.
- I will not post negative comments about the school or staff on social network sites.
- I will not complete and send forms without permission from my teacher.
- I will not give out any personal information such as name, phone number or address and will not use the ICT system to arrange to meet someone.
- I understand that all my use of the Internet and other related technologies is monitored and logged and can be made available to my teachers or parents/guardian.
- I understand that personal files stored on the network services may be checked by others including teachers and authorised members of the system support team.
- I will not attempt to access the school network system using unauthorised equipment or attempt to access restricted areas of the system to which I should not have access under the restrictions of my network account.
- I understand that that these rules are designed to keep me safe and if not followed, sanctions will be applied to my account.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school. I have read and understood the e-Safety Policy.

Signature …… Date ……

Full Name …….... (printed)

Appendix 2

Staff Acceptable Use Policy / Code of conduct

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school.
This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school e-Safety coordinator.
Failure to follow this policy may result in disciplinary action in accordance with the school's e-safety policy.

- I will only use the school's email / Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only access the computer system with the login and password I have been given
- I will not access other network user's files unless specifically authorized to do so
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on CMIS) is kept secure and is used appropriately, whether in school, or accessed remotely.
- I will not post negative comments about the school or staff on social network sites.
- I will not browse, download or upload material that could be considered offensive or illegal.
- I will not send to pupils or colleagues material that could be considered offensive or illegal
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software.
- I will not allow unauthorised individuals to access email / Internet / Intranet.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school. I have read and understood the e-Safety Policy.

Signature …… Date ……

Full Name …….. (printed)

Job title . . . . . .

Appendix 3

Guidance: What to do if?

e-Safety Co-ordinators: **Mrs A.Ager – Deputy Head**
Mr P. Aulton – Asst, Head
Miss H. Nicholls – Asst Head

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child

1. Play the situation down: don't make a drama.
2. Report to the headteacher/e-Safety co-ordinator who will decide whether to inform parents of any children who viewed the site.
3. Inform the school's ICT service and ensure the site is filtered.

An inappropriate website is accessed <u>intentionally</u> by a child

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents/guardian of the child.
3. Inform the school technicians and ensure the site is filtered if need be.

An adult uses School IT equipment inappropriately

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Headteacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal.
   The headteacher or nominee should then:
   - Remove the PC to a secure place.
   - Instigate an audit of ICT equipment by the school's ICT Network Manager to ensure there is no risk of Pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (following the school's disciplinary policy).
4. In an extreme case where the material is of an illegal nature the Headteacher should then:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - Inform Management Support.
   - If requested, remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time

- Inform the Progress Leader or School e-Safety co-ordinator.
- Advise the child not to respond to the message.

The Progress Leader will then:

- Refer to relevant policies including e-Safety, anti-bullying and apply appropriate sanctions.
- Secure and preserve any evidence.
- Notify parents of the children involved and encourage them to report the incident to the police

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff

If the comments have come from an external source, report the incident to the e-Safety co-ordinator who will:

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Endeavour to trace the origin and inform the police as appropriate.

If the comments have come from an internal source: Refer to e-Safety co-ordinator for investigation.

The e-Safety co-ordinator will then:

a) Refer to acceptable user policy that was signed by the child, and apply agreed sanctions.
b) Notify parents of the child responsible/child affected by comments.
c) Inform the school technician and ensure all evidence is secure and preserved.
d) Consider the involvement of the police.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with a child

1. Report to and discuss with the named child protection officer/e-Safety co-ordinator.

The e-Safety co-ordinator will then:

a) Advise the child on how to terminate the communication and save all evidence.
b) Follow safeguarding procedures
c) Contact the 'protect team'

All of the above incidents must be reported immediately to the Headteacher and e-Safety co-officer.

Children should be confident that when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.