Cranmore Infant School

Acceptable user and E-Safety Policy – January 2014

'The internet can be extremely beneficial for children; they can use it to learn, communicate, develop, create and explore the world around them. However, too often, it also leaves them vulnerable to risks and exposes them to experiences which they find upsetting. These online risks are not always fully understood but it is essential for children's safety that they are addressed. For many children a distinction between their online and offline lives does not exist' **(How safe are our children? NSPCC 2014)**

Vision

Cranmore Infant School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies such as games consoles, tablets and mobile phones. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Cranmore Infant School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed, wireless and mobile technologies owned and supplied by the school and to personal devices owned by adults and children while on the school premises.

Our Acceptable Use and E-safety Policies have been written for the school, building on the Solgrid E-safety policy, the WMnet policy, Becta and government guidance. It has been agreed by the senior management and approved by governors on _____. It will be reviewed annually.

Created by: Carol Baker / Laura Rushton

Date: November 2014

To be revised: November 2015

Approved by the Governors _____-

Contents

Introduction

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

The Green Paper Every Child Matters and the provisions of the Children Act 2004, Working Together to Safeguard Children set out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:
• safe from maltreatment, neglect, violence and sexual exploitation
• safe from accidental injury and death
• safe from bullying and discrimination
• safe from crime and anti-social behaviour in and out of school
• secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of our school to ensure that every child in their 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.

The whole school ensures they keep up to date with e-Safety issues with help from the ICT lead and the leadership team who receive guidance through liaison with the Local Authority e-Safety Officer and through organisations such as The Child Exploitation and Online Protection (CEOP). Governors are updated by the Head teacher or the ICT lead.

Technologies

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet on a variety of devices
- E-mail & Instant messaging
- Learning Platforms and Virtual Learning Environments
- Wikis
- Social networking sites
- Gaming Sites
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality

Roles and Responsibilities

At Cranmore we take a whole school approach to e-safety by creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-safety education programme for pupils, staff and parents

The Head teacher and Governing body have ultimate responsibility for enforcing and establishing acceptable and safe practice and managing e-Safety issues at our school. The staff are aware that they need to report any e-Safety issues to the Head teacher, our designated senior person for child protection and member of the senior management team. They are the central point of contact for all e-Safety issues and will be responsible for day to day management alongside ICT/computing subject leader. The school has established an e-Safety committee that are responsible for policy review, risk assessment, and e-safety in the curriculum. The current members are: The Head Teacher, The Deputy Headteacher, ICT/computing subject Leader. We also ask for updates and advice from our ICT Technician whom we employ through EICTS (Education ICT services Solihull) and from the Synergy cluster group when training and updates are given. Staff are aware that e-Safety is a whole school responsibility.

All members of the school community have certain core responsibilities within and outside the school environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Additional roles and responsibilities are discussed in the Becta document - AUP's in context: Establishing safe and responsible behaviours and also available at https://www.solihull.gov.uk/Attachments/e-safetycurriculum.pdf.

These will be communicated to the relevant groups at appropriate times.

Physical Technical Infrastructure and Environment / Security

The school endeavours to provide an acceptable and safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

In our school:

- EICTS provide the school with internet access and maintains the system.
- Anti-virus software is provided and installed by EICTS on all computers and updated regularly
- Central filtering is provided and managed by Solihull EICT services. All staff and pupils are taught that if an inappropriate site is discovered it must be reported to their class teacher and the ICT/computing subject leader or The Headteacher who will report it the to the Solihull EICT Service Desk to be investigated where necessary and blocked. All incidents will be recorded in the e-Safety log for audit purposes.

- Requests for changes to the filtering will be directed to The ICT Subject leader in the first instance who will forward these on to Solihull. Change requests will be recorded in the e-Safety log for audit purposes
- There are restrictions on certain sites such as 'You tube' where only staff have access to this and are told to watch first to see if it is appropriate before children watch it for educational purposes
- The only social networking site that can be accessed in school is twitter however staff understand that they are not to access this for personal use at any time on a school computer.
- The school has a facebook and twitter page specifically for current parents only to update them on school events. This is monitored closely by the ICT lead.
- We have a separate server in the school which is dedicated to 'Espresso' that is housed in the main comms cupboard.
- Pupil use is monitored by class teachers and The ICT/computing subject leader
- Staff use is monitored by the Headteacher and the ICT/computing Subject leader
- All staff (and regular supply staff) and school governors are issued with their own username and password for school network access. Visitors/Supply staff and student teachers will be issued with temporary ID's and the details recorded in the ICT log folder in the work room. They will also be made aware of this policy and asked to abide by it and sign the policy.
- All pupils have their own username and password and understand that this must not be shared and they sign along with their parents to be responsible users both at home and school

Mobile / emerging technologies

- Teaching staff at the school are provided with laptop usage in school and for use where necessary outside of school for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times. Some staff also have 'remote access' to the school network which has 2 part security set up and monitored by EICTS.
- To ensure the security of the school systems and personal data, personal laptops/tablets are currently not permitted to be used in school or connected to the school network. Personal equipment such as memory sticks, cameras or SD cards should also not be used in school. We have provided staff with cameras and password protected/encrypted memory sticks only these should be used be used unless permission is gained from the ICT/computing subject leader or technician and the equipment virus checked. No software should be added to the computer or network without permission from the ICT subject leader or technician.
- Staff understand that they should only use their own mobile phones in their own time and be locked securely away at all other times and in line with the school Safeguarding policy. School mobile phones are available for any off site trips for emergency communication only.
- Parents are asked not to use any mobile devices when accompanying classes on school trips.
- Children are not allowed any camera usage of their own on trips or in school.
- Pictures / videos of staff and pupils should not be taken on personal devices. Use of school cameras is allowed but only to be saved on the school network and used publically with the child's parental consent.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community
- If any Visitors or speakers come to school they must email any presentations etc. beforehand or ask before any technical equipment is to be used.
- Parents are only allowed to post pictures of their own child on social networking sites and this message is relayed to them at every significant school event.

E-mail

The school e-mail system is provided, filtered and monitored by ICT Services and is governed by Solgrid (Solihull Council E-mail Use Policy).

- **Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication**

- All staff and governors are given a school e-mail address and understand that this one must be used for all professional communication
- The pupils are given a school e-mail address that can be used for educational activities
- Guidance is given to the school community around how e-mail should be structured when using school e-mail addresses
- Staff are allowed to access personal e-mail accounts on the school system **outside** directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software
- Everyone in the school community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety co-ordinator as soon as possible
- Staff will not open attachments from an untrusted source and will inform the e-safety co-ordinator if they receive an offensive e-mail.

Pupils

- Pupils are introduced to email as part of the ICT Scheme of Work.
- Pupils may only use the school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils can only use school domain e-mail accounts on the school system.
- Pupils must immediately tell a teacher / trusted adult if they receive an
- offensive e-mail.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone. This is taught explicitly through e-safety lessons across the school.

Published content and Digital Media

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed on school websites or outside the school.

The Head teacher takes responsibility for content published to the school web site but delegates general editorial responsibility to The ICT subject leader. Class teachers and subject leaders are responsible for the editorial control of work published by their pupils on the extranet.

- The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The school encourages the use of e-mail to contact the school via the school office / generic e-mail addresses / staff e-mail addresses
- The school does not publish any contact or personal details for the pupils

Safe Use of Images

- Digital images are easy to capture, reproduce and publish and, therefore, misuse.
- There are strict guidelines applying to images, digital or otherwise, being used on school premises.

Using Images and Film

On a child's entry to the school we gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form. We as a school will ask for permission to use digital images For instance:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes recorded/transmitted on a video or webcam general media appearances,

e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).
- Photographs will be published in line with Becta guidance and not identify any individual pupil
- Students' full names will not be published outside the school environment

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. The parent/carer should notify the school if there is any such change in circumstances and they may withdraw permission, in writing, at any time. Equally they may decide to place in writing so that images of children will not be used in school whatsoever. We also ask the parents that no photos/videos are placed on the internet if they record any school events/assemblies etc. This is monitored as much as possible by the ICT lead using the school facebook page,

Storage of Images and Film

Digital images /videos of pupils are stored in the staff shared area on the network and images are kept for one full year after the academic year ends – unless an item is specifically kept for a key school publication or historical archive.
Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network
Class teachers have the responsibility of deleting the images when they are no longer required or the pupil has left the school.

Social Networking and online communication

The school does not allow access to any commercial social networking sites. However we have a facebook page specifically for current parents only to update them on school events. This is overseen by the Headteacher, ICT/computing subject leader and updated by a designated member of staff (currently LR)

We have a Solgrid Extranet site, which is password protected is available to pupils in school and at home where parents and pupils have signed the AUP policy.

The only social networking site that can be accessed in school is twitter however staff understand that they are not to access this for personal use at any time on a school computer. Guidance is regularly provided to the school community on how to use social network sites safely and appropriately out of school to protect them where necessary.

If any teacher is made aware that a child in our school holds a social network account this is to be reported and investigated and recorded in the incident log with any action necessary.

Educational Use

School staff model appropriate use of school resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material. **This is especially important when using resources such as 'google' and other search engines.**
- Where appropriate, links to specific web sites will be provided instead of open searching for information
- Pupils will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers

- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity
- All users must observe software copyright at all times. It is illegal to copy or distribute school software of illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

E-safety training

ICT and online resources are increasingly used across the curriculum. At Cranmore we believe that it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded into the curriculum and ensures that every pupil is educated about safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.

The school has a framework for teaching internet skills in ICT / PSHE lessons.
The school provides opportunities within a range of curriculum areas to teach about e-safety.
Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the safety curriculum.
We have Assemblies on E-Safety where necessary and appropriate which parents are also invited too.
Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
Pupils are made aware of the impact of online bullying through PSHE (Personal, Social & Health Education) and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT/computing curriculum.

The school will assess and support staff skills and have a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.

- E-safety training will be made part of the induction process and mentor scheme available for new members of staff.
- Educational resources are reviewed by The ICT subject leader and disseminated through curriculum meetings / staff meetings / training sessions

Parental Involvement

- We believe that it is essential for parents / carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss safety with parents / carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.
- The school will disseminates information to parents relating to e-safety where appropriate in the form of:
- Information evenings
- Posters
- Website / Fronter postings
- Newsletters
- Parents / carers will receive a copy of the acceptable use policy which needs to be read with their child, signed and returned to the school confirming both an understanding and acceptance of the rules. The school will keep a record of the signed forms.
- Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g. on school website).
- A partnership approach with parents will be encouraged.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998

Data is stored on the school systems and transferred in accordance with the Becta Data Security Guidelines. Staff are made aware that pupils personal data should not be stored on personal equipment and they should only use the encrypted and password protected resources that are provided at school to stop any data being lost or stolen.

Responding to incidents

Inappropriate use of the school resources will be dealt with in line with other school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police. The ICTS Service Desk will also be informed to ensure that the Local Authority can provide appropriate support for the school
- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Head
- Breaches of this policy by staff will be investigated by the headteacher. Action will be taken under Solihull Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring of staff use will be carried out by at least 2 senior members of staff.
- Pupil policy breaches relating to bullying and abuse of the system must be reported to the nominated child protection representative and action taken inline with school anti-bullying and child protection/Safeguarding policies. There may be occasions when the police must be involved.
- Minor student offenses, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.
- Any incidents are logged on the W-drive and recorded in the head teacher's safeguarding folder.

Writing and Reviewing this Policy

- There will be an ongoing opportunity for staff to discuss with the e-safety coordinator any issue of e-safety that concerns them. They will be given opportunities to be involved in the making and reviewing of this policy and AUP through consultation and amending initial drafts.
- This policy will be reviewed as part of the school's rolling programme and consideration will be given to future whole school development and new technologies.

Cranmore Infant School.

Acceptable Use Policy (AUP)

The following points underpin the AUP for Cranmore Infant School:

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT subject leader.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils will not be allowed access to public or unregulated chat rooms.
- The school will work in partnership with parents, the LEA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT subject leader or the ICT technician.
- Rules for Internet access will be posted in all rooms where computers are used. This will inform pupils that Internet use will be monitored. Instruction in responsible and safe use should precede Internet access.

Staff, Governors and Visitor

Acceptable Use Policy

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher or ICT/computing Subject leader.

This policy covers the use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not disclose any passwords provided to me by the school or other related authorities and if my passwords are compromised, I will ensure that I change it.
- I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved school email or other school approved communication systems for school business including that with pupils or parents/carers, and only communicate with them on appropriate school business. (The current e-mail system is: solgrid staff mail)
- I will not browse, download or send material that could be considered offensive, illegal or discriminatory.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended antivirus, firewall and other ICT 'defence' systems.
- I understand that Images of pupils will only be taken, stored and use for professional purposes inline with school policy and with written consent of the parent or carer. Images will not be taken using a personal digital camera or camera phone and will not be distributed outside of the school network without the permission of the parent or carer.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role and will not bring not bring my professional role into disrepute.
- 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 issues that may occur with it.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be

kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager or Head teacher on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I agree to abide by all the points above.
I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

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

Full Name ..... (printed)

Job title .....

School .....Cranmore Infant School.....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

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

Cranmore Infant School

AUP for pupils.

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate to my work at the time
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- only email people I know or those approved by a responsible adult
- only use email which has been provided by school when in school
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me

I know that once I post a message or an item on the internet then it is completely out of my control. I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

Signed: _____

Safety

WMnet (wmnet.org.uk) has a very comprehensive section on their website which covers elements of e-safety for children, teachers *and* parents that includes safe search engines and image searches for children to use at home and at school. This link is for teachers:
http://www.wmnet.org.uk/21.cfm?zs=nb - Thinkuknow E-Safety resources
New to this site are the 'Thinkuknow' materials which are suitable for all year groups. This link is for staff and pupils and takes you straight to the new materials:
http://www.thinkuknow.co.uk/5_7/

Websites to teach E-Safety:
http://www.thinkuknow.co.uk/5_7/
More FKS year 1 - http://www.thinkuknow.co.uk/5_7/leeandkim/default.aspx
Year 1/2 http://www.thinkuknow.co.uk/5_7/hectorsworld/

http://www.bbc.co.uk/cbbc/help/safesurfing/index.shtml**)**

For Adult information and safety
http://www.thinkuknow.co.uk/11_16/

General:
http://www.bbc.co.uk/cbbc/help/safesurfing/index.shtml
http://www.childnet-int.org/projects/
http://www.nextgenerationlearning.org.uk/safeguarding (for teachers and parents)

Recommended 'Safe Search' sites:
http://www.askkids.com/
http://kids.yahoo.com/

'Safe Image' sites:
WMnet safe images:
http://www.wmnet.org.uk/wmnet/index.cfm?p=292,index&zz=20081105151930474

http://gallery.nen.gov.uk/
http://ngfl.northumberland.gov.uk/clipart/

Cranmore Infant SchoolE-safety Incident Log

Date and Time	Name of pupil or staff member	Male or female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.
1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (report to EICTS).

An inappropriate website is accessed intentionally by a child.
1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform EICTS.

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 head teacher and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the PC to a secure place.
    - Instigate an audit of all ICT equipment by the schools ICT managed service providers 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 (contact Personnel/Human Resources).
    - Inform governors of the incident.

4. In an extreme case where the material is of an illegal nature:
    - Contact the local police or High Tech Crime Unit and follow their advice.
    - If requested to 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.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PSHE and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents of the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform the LA e-safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.
1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA e-safety officer.
The school may wish to consider delivering a parent workshop for the school community

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Photograph, Video & Website Permission

Please complete and return to school immediately

Name……Year……..

I give permission for photographs and/or videos to be taken in the following situation:

Photographs

	Yes	**No**
Taken by school staff to be used only in school		
Taken by students/LEA here who require photographs for their project work or publications		
Taken by the press for use in publications such as newspapers or educational material		
Taken by school staff for use in training sessions or school documents		

Videos

	Yes	**No**
Filmed by school staff to be used in school to give information for children's records etc		
Taken by staff for use in training sessions in school or with other professionals i.e. LEA, students		
Taken by professional/amateur film makers to be used for training school staff or practioners in other settings (may be used with other professionals and parents)		

School Website

	Yes	**No**
Photograph or filmed by school staff for use on school website / open to public viewing		

Fronter

	Yes	**No**
Photograph or filmed by school staff for use on school website. These can only be accessed by school families with username & passwords		

Signed……..Date……