Rosebank School

Learning together, celebrating success

e-SAFETY IN SCHOOL POLICY

DATE OF THIS POLICY:	**DECEMBER 2015**
Ratified by Governors:	FGB 10.12.15
Frequency of update:	Annually
Due for revision:	**DECEMBER 2016**
Person responsible:	Natasha Tompkins

ROSEBANK SCHOOL

e-SAFETY IN SCHOOL POLICY

RATIONALE

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

e-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

WHY IS INTERNET USE IMPORTANT?

Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is an essential element of life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff, to enhance the school's management functions and business administration systems.

HOW DOES INTERNET USE BENEFIT EDUCATION?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support;
- Exchange of curriculum and progression data;
- Access to learning wherever and whenever convenient.

HOW CAN INTERNET USE ENHANCE LEARNING?

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights and the correct use of published material should be taught where appropriate.

The school's Internet access will be designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils comply with copyright law.

Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

Pupils will be educated throughout the school year in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation where appropriate.

Pupils will be taught, throughout the year, to acknowledge the source of information used and to respect copyright when using Internet material in their own work where appropriate.

HOW WILL PUPILS LEARN HOW TO EVALUATE INTERNET CONTENT?

Information received via the Internet, email or text message requires good information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read.

Researching potentially emotive themes such as the Holocaust as part of a World War 2 theme can provide an opportunity for pupils to develop skills in evaluating Internet content.

Pupils will use ability and age-appropriate tools to research Internet content. The evaluation of online materials is a part of teaching and learning in all topics where the age and ability of the pupil render it appropriate.

HOW WILL INFORMATION SYSTEMS SECURITY BE MAINTAINED?

- Servers are located securely and physical access restricted.
- The server operating system will be secure and kept up to date.
- Virus protection for the whole network is installed and current.
- Access by wireless devices is proactively managed and secured.
- The security of the school information systems and users is reviewed regularly.
- Virus protection is updated regularly.
- Personal data sent over the Internet or taken off site must be encrypted.
- Portable media may not be used without permission, this will be password protected where possible.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Computing Subject Leader and network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

HOW WILL EMAIL BE MANAGED?

Email is an essential means of communication for both staff and pupils. However, unregulated email can provide routes to pupils that bypass the traditional school boundaries.

In the school context (as in the business world), email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work-provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

Email accounts should not be provided which can be used to identify both a student's full name and their school. Instead, whole-class or project email addresses should be used. When using external providers to provide students with email systems, schools must pay close attention to the site's terms and conditions as some providers have restrictions of use and age limits for their services.

- Pupils may only use approved email accounts for school purposes;

- Pupils must immediately tell a designated member of staff if they receive offensive email;

- Pupils must not reveal personal details of themselves or others in email communication;

- Whole–class or group email addresses will be used for communication outside of the school;

- Staff will only use official school-provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team;

- Email sent to external organisations should be written carefully and authorised before ending, in the same way as a letter written on school headed paper would be;

- The forwarding of chain messages is not permitted;

- Staff should not use personal email accounts during school hours unless permission has been given from Senior Leadership Team, with the exception of personal mobile phones which may be used during breaks and at lunchtimes in the staff room.

HOW WILL PUBLISHED CONTENT BE MANAGED?

The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information must not be published.

The Computing Subject Leader, Head Teacher and website assistant will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

Photographs included on the website will be selected carefully.

Pupils' full names will not be used on the website in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on websites.

Photographs will be resized before being published on the website to reduce the risk of digital manipulation.

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests.

Users can be invited to view personal spaces and leave comments, over which there may be limited control.

All staff should be made aware of the potential risks of using social networking sites personally (outside of school and outside of school hours). They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs, etc.

Pupils will not access Social Media sites in school and online chat is not permitted in school.

Pupils will be taught about how to keep personal information safe as part of the e-safety programme.

HOW WILL FILTERING BE MANAGED?

Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily after permission is granted by the Senior Leadership Team.

Systems to adapt the access profile to the pupil's age and maturity are available including class passwords.

The school's broadband access will include filtering appropriate to the age and maturity of pupils.

The school has a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Subject Leader who will then record the incident and escalate the concern as appropriate.

Any material that the school believes is illegal will be reported to appropriate agencies such as Cheshire Police or CEOP (Child Exploitation and Online Protection Centre).

The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

HOW ARE EMERGING TECHNOLOGIES MANAGED?

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers.

Schools should keep up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies.

Staff will not contact pupils or parents using personal mobile phones; school-owned phones are available at all times including for educational visits. Please also refer to the Acceptable Use of Communications Policy.

The inclusion of inappropriate language or images is difficult for staff to detect. Pupils may need reminding that such use is inappropriate and conflicts with school policy. Abusive messages should be dealt with under the school's Anti-Bullying policies and will involve if necessary, Cheshire Police.

Emerging technologies will be examined for educational benefit and a discussion with the e-Safety Subject Leader and SLT will be carried out before use in school is allowed.

Parents will be invited to attend e-safety sessions in school, and have a chance to share their experiences and discuss strategies that can be used at home.

Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

HOW SHOULD PERSONAL DATA BE PROTECTED?

While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Held no longer than is necessary;
- Processed in line with individual's rights;
- Kept secure;
- Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

POLICY DECISIONS

Students will not be granted access to the Internet unless the parents have signed a parent consent form.

All staff will read and sign the Acceptable Use Policy before using any school Computing resources.

All visitors to the school site who require access to the schools network or Internet access will be asked to read and sign an Acceptable Use Policy.

Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.

Pupils will be supervised on the Internet and using other technologies at all times.

Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

HOW WILL RISKS BE ASSESSED?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.

Neither the school nor Cheshire West and Chester Council can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit Computing use to establish if the e–Safety Policy is adequate and that the implementation of the e–Safety Policy is appropriate.

The use of computer systems for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Cheshire Police.

Methods to identify, assess and minimise risks will be reviewed regularly.

HOW WILL THE SCHOOL RESPOND TO ANY INCIDENTS OF CONCERN?

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, and illegal content).

The e-Safety Subject Leader will record all reported incidents and actions taken in the School e-Safety Incident Log and in any other relevant areas e.g. Bullying or Child Protection Log.

The Designated Child Protection Lead will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.

The school will manage e-Safety incidents in accordance with the school Behaviour Policy and Anti-Bullying Policy where appropriate.

The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team.

HOW WILL E–SAFETY COMPLAINTS BE HANDLED?

Complaints about Internet misuse will be dealt with under the school's Complaints Procedure.

Any complaint about staff misuse will be referred to the Headteacher.

All e–Safety complaints and incidents will be recorded by the school, including any actions taken.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

HOW WILL CYBER-BULLYING BE MANAGED?

> Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.
>
> *(DfE, October 2014)*

> Cyber-bullying is when one person, or a group of people, try to threaten or embarrass someone else using a mobile phone or the internet.
>
> *(Gov UK, 2012)*

> Cyber-bullying is the use of Information Communication Technology, particularly mobile phones and the internet, deliberately to upset someone else. Cyber-bullying may consist of threats, harassment, embarrassment, humiliation, defamation or impersonation. Cyber-bullying may take the form of general insults or prejudice-based bullying, for example homophobic, sexist, racist or other forms of discrimination.
>
> *(Digizen, 2009)*

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents;
- Gives Headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it should be investigated and acted on.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986.

Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's Anti-Bullying Policy.

All incidents of cyber-bullying reported to the school will be recorded.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber-bullying and the school's e-Safety ethos.

Parent/carers of pupils will be informed.

The Police will be contacted if a criminal offence is suspected or if deemed necessary.

HOW WILL MOBILE PHONES AND PERSONAL DEVICES BE MANAGED?

The use of mobile phones and other personal devices by students and staff in school is covered in the school Acceptable Use of Communications Policy.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school Behaviour and Anti-Bullying Policy.

School staff may confiscate a phone or device if they believe it is being used to contravene the school's Behaviour or Anti-Bullying Policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence, the phone will be handed over to the police for further investigation.

- **Pupils' Use of Personal Devices**

If a pupil breaches school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released at the end of the school day.

Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

- **Staff Use of Personal Devices**

Unless with prior consent from a member of the Senior Leadership Team, mobile phones and personal devices will not be used during teaching hours. They should be switched off and placed in a secure environment.

Staff personal phones are not to be used in the reception foyer or corridors. They may be used in the staffroom during breaks and at lunchtimes.

Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

Staff will be issued with a school phone where contact with pupils or parents/carers is required.

Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action may be taken.

HOW WILL THE POLICY BE INTRODUCED TO PUPILS?

All users will be informed that network and Internet use will be monitored.

An e–Safety training programme of stand-alone lessons/assemblies will be established across the school, as set out in the new 2014 Computing curriculum, to raise the awareness and importance of safe and responsible Internet use amongst pupils.

An e–Safety module will be included in the PSHCE Scheme of Work and as part of the Computing Scheme of Work, which will look at who we can trust when using the Internet, and what information we should be careful about giving out when looking at using the Internet as a learning tool.

e-Safety rules ('Our Internet Rules') will be posted in all rooms with Internet access.

Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Particular attention to e-Safety education will be given where pupils are considered to be vulnerable. This is in line with Keeping Children Safe in Education 2014: giving children opportunities to learn about safeguarding.

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www1.orange.co.uk/education
- Safe: www.safesocialnetworking.org

HOW WILL THE POLICY BE DISCUSSED WITH STAFF?

The e–Safety Policy will be formally provided to and discussed with all members of staff.

To protect all staff and pupils, the school will implement Acceptable Use policies.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

HOW WILL PARENTS' SUPPORT BE ENLISTED?

Parents' attention will be drawn to the school e–Safety Policy in newsletters, and on the school website.

A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering sessions with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. Parents' Evenings and sports days.

Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.

Information and guidance for parents on e–Safety will be made available to parents in a variety of formats including leaflets and training.

Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.

e-Safety Contacts and References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

APPENDIX 1

NOTES ON THE LEGAL FRAMEWORK

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It should not be taken as advice on legal issues.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the Internet.

Racial and Religious Hatred Act 2006

This Act makes 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.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

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). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust (typically, teachers, social workers, health professionals, etc.)

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.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

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 someone else's password to access files);
• gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
• impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

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

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (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.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. 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.

It is an infringement of copyright 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.

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.

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against them 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.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication.

The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Criminal Justice and Immigration Act 2008

Section 63: it is an offence to possess an "extreme pornographic image".

63 (6) must be "grossly offensive, disgusting or otherwise obscene".

63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" which must also be "explicit and realistic".

Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyber-bullying/Bullying:

• Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
• School staff are able to confiscate items such as mobile phones, etc when they are being used to cause a disturbance in class or otherwise contravene the school Anti-Bullying Policy.

Dear Parents,

Responsible Internet Use

As part of your child's curriculum and the development of their Computing skills, Rosebank School provides supervised access to the Internet. We believe that effective use of the web and e-mail is an essential skill for children growing up in the modern world. All pupils learn about e-safety and follow our Internet rules (written with input from the School Council) to keep themselves safe online. These rules are displayed throughout school and in all classrooms.

Although there are concerns about pupils having access to undesirable materials we have taken positive steps to reduce the risk in school. Our school Internet provider, Cheshire West and Chester, operates a filtering system to restrict access to inappropriate sites and content.

Every effort is made to ensure that pupils' access to the Internet is suitable and appropriate. However, the school cannot be held responsible for the content of materials accessed through the Internet. The school will not be liable for any damages arising from any child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please contact the school to arrange an appointment with the Headteacher.

Please read, sign and return the attached Internet Access and ICT Use for Pupils form as soon as possible.

Yours sincerely,

APPENDIX 3

Rosebank School

RESPONSIBLE INTERNET ACCESS AND COMPUTING USE FOR PUPILS PARENT CONSENT FORM

Children have the opportunity to use the Internet and electronic mail in school.

Please read the school "Policy for Acceptable Use of Communications and Information" and "School e-Safety Policy" available on our website www.rosebank.cheshire.sch.uk

Please explain the meaning of these policies and the school rules on the use of the Internet and Computing in school to your child.

Please complete the form below, sign it and return it to school as soon as possible.

Please note: No pupil will be granted access to the Internet unless we have a parent consent form.

Parent name .....

- I have read and understood the school rules for responsible Internet use and give permission for my child to access the Internet.
- I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.
- I understand the school cannot be held responsible for the nature or content of materials accessed through the Internet.
- I agree that the school is not liable for any damages arising from use of the Internet facilities.
- I have read the relevant policies stated above and explained their meaning to my child.

Parent signature ..... Date .....