Revised Standard Circular 69
August 2009

East Renfrewshire Council: Education Department

Council Offices
211 Main Street
Barrhead
East Renfrewshire
G78 1XB

To Heads of All Educational Establishments

Dear Colleague

REVISED STANDARD CIRCULAR 69

GUIDELINES ON THE SAFE USE OF THE INTERNET, ELECTRONIC COMMUNICATIONS AND MOBILE TECHNOLOGIES

Contents

1. Introduction
2. Background
3. Guidance on the Safe Use of the Internet and Electronic Communications and Mobile Technologies
4. The Role of the Authority
5. The Role of the ERC ICT Network Team
6. The Role of the School
7. The Role of the ICT Co-ordinator
8. The Role of Parents or Carers
9. Communication Applications
10. Mobile Technologies
11. Conclusion

Appendix 1 Responsible User Agreements – Secondary Pupils, Primary Pupils, Parent/Guardian Information

Appendix 2 Relevant Websites

Appendix 3 The Use of Mobile Technologies within Educational Establishments

EAST RENFREWSHIRE COUNCIL: EDUCATION DEPARTMENT

GUIDELINES ON THE SAFE USE OF THE INTERNET, ELECTRONIC COMMUNICATIONS AND MOBILE TECHNOLOGIES

1. Introduction

"There is no doubt that Information and Communications Technology (ICT) can bring benefits to young people and enhance their learning experience. The vast array of information, often from the original source, and the instantaneous communication using a variety of media will change the way we experience life and work. It is essential that young people have the opportunity to experience these new technologies and to develop the communication, searching, sorting and filtering skills that are likely to be part of their everyday life.

Nevertheless, this same ability to access information on almost any subject, and to communicate throughout the world, carries with it the risk that young people will be exposed to material, situations or communications that are undesirable."

DoubleClickThinking: Personal Safety on the Internet (2003)

2. Background

In 1999 SOEID published "*ClickThinking: Personal Safety on the Internet*" in recognition of the potential risks associated with access to the Internet. As there have been a number of developments in application packages, local area networks, modes of communication, volume of electronic communication, speed and availability of access which have changed the nature and significance of the Internet and other electronic communications technologies, the Scottish Government updated the original guidance in March 2003. This updated guidance is available on a single website http://www.ltscotland.org.uk/doubleclickthinking/ which provides advice and links to a number of national and international resources regarding child safety on the Internet.

This online publication is designed to minimise risks associated with Internet access and other electronic communications within Education Authorities and schools.

The following guidance draws together the recommendations within not only this updated publication but also policy documentation and advice already available within the authority, with the purpose of offering clear guidance on the safe use of the Internet, electronic communications and mobile technology both at local authority and school level, indicating the responsibilities of the various users of the East Renfrewshire Education Network.

3. Guidance on the Safe Use of the Internet and Electronic Communications and Mobile Technologies

As stated in the *"Policy for the Development of Information and Communications Technology (ICT) within Educational Establishments" (March 2001)*, East Renfrewshire Council Education Department, in seeking to promote the use of ICT within the Education Department, aims to:

- ensure that all young people have the opportunity to become skilled with the tools of information and communication technologies in all establishments in a safe and secure environment;
- ensure that the potential of ICT is maximised to the benefit of learning and teaching at all stages and in all sectors; and
- ensure that ICT tools are used to support effective management and administration in all establishments in the education department.

East Renfrewshire Council is determined to work with parents and other agencies to ensure that students use the Internet, electronic communications and mobile technology safely and are protected from unsuitable material and inappropriate contact. To do this we have produced these guidelines, which makes clear the role of the authority, the school, the parents and the pupils in reducing any risks associated with Internet access.

4. The Role of the Authority

The role of the Authority and that of schools in meeting the above aims are outlined in great detail within the above mentioned policy document. Those which are directly related to safety are listed below:

The Authority will:

- ensure that the network and its components provide a secure environment for all users;
- ensure that the network is protected from internal and external misuse;
- install and maintain network security systems;
- maintain and modify access rights of pupils and teachers to network resources;
- ensure that access to Internet is restricted according to pupil age to ensure that inappropriate materials are not available through the network;
- install and maintain network monitoring software; and
- develop codes of practice for the use of the network users.

The majority of these safety-related aims are the responsibility of the ERC ICT Network Team in the Finance Department's E-Government section.

These measures relate specifically to the Internet, electronic communication and mobile technologies, but the Council also has a Child Protection Policy that deals with any issues where there is a concern about the possibility of any form of child abuse. All policies and procedures to do with Internet Safety are subject to the more strategic measures in the Child Protection Policy.

The Child Protection Committee has developed and distributed leaflets for safe access to the Internet for both children and parents. The Committee also developed a web site to provide information to the general public on safety aspects of the Internet.

All Council premises for young people have established protocols for safe access to the Internet and a number of national leaflets are available for guidance in relation to safe use.

The Education Department's ICT Central Technician Service ensures that all systems connected to the Education Network have anti-virus software installed to identify and protect against programs that could make changes to the computer system. Updates to the anti-virus software are downloaded on an hourly basis and when a user logs on to a workstation.

East Renfrewshire Council's Education Department's Standard Circular 78, *"Use of Information Technology Equipment and Systems Connected to the Education Network" (September 2002)* establishes a clear policy for all employees in schools and other establishments with regard to access to PCs, other ICT equipment and systems and Internet and e-mail use.

The *"Policy for the Development of Information and Communications Technology (ICT) within Educational Establishments" (March 2001)*, notes that schools will require to construct their own policy covering the development of ICT within each establishment. **This documentation will need to be updated regularly to take account of new developments.** Responsible User Agreement templates for both primary and secondary pupils are attached as Appendix 1

to this guidance. Schools are welcome to use none, any or all of the appropriate template to construct their own Responsible User Agreements.

5. The Role of the ERC ICT Network Team

As stated in the "Education Network Maintenance and Development Strategy April 2003-March 2006", it is the role of the ERC ICT Network Team to ensure that the security procedures in place for the Education Network conform to Council standards.

The technological solutions used by the ERC ICT Network Team to form part of a consistent strategy to provide safe Internet access include:

- A firewall to prevent unauthorised access from outwith the local network;
- User authentication software to ensure that only recognised users are allowed access to the system via password;
- Web filtering and blocking software to prevent access to certain services. The Network Filtering Policy currently in place outlines those categories of services currently blocked. The policy is updated to address issues raised by audit, including improvements to physical security in schools, increased protection of the Corporate Network in certain areas, and a review of remote access procedures. The filtering system in place can be tailored to meet the needs of different user groups. Any member of staff can request that a web address be unblocked for either staff or staff and pupil use. All such requests are copied to the ICT coordinator for information. As this method of access circumvents the normal filtering process the contents of these sites will be viewed by the ERC ICT Network Team, and action predicated on the result;
- Internet access monitoring software to provide reports about attempted violations of use;
- E-mail monitoring software to identify inappropriate content and use.

The nature of actions to be taken when policies are breached is devolved to the school, although the right to raise complaints to a higher level including the police is reserved. On request of a school's ICT Coordinator or their representative, any user can be denied access to all or some facilities, with access being returned on request. The ERC ICT Network Team will assume that disciplinary action has been carried out to the school's satisfaction. Any individual who considers that they have been subject to unacceptable behaviour is entitled to make a complaint. In serious circumstances the ERC ICT Network Team reserves the right to suspend access to any user without prior consultation. The Head Teacher/ICT coordinator will be advised of such action immediately.

6. The Role of the School

The role of school in meeting those aims directly related to safety as stated in the *"Policy for the Development of Information and Communications Technology (ICT) within Educational Establishments" (2001)*, are listed below:

Schools will:

- develop an establishment policy encompassing the use of ICT in the curriculum, learning and teaching and administration;
- make arrangements so that the network and its facilities are not misused by any user;
- ensure that the use of the network and its ethical use are discussed with all users and parents of pupils below statutory age.

Therefore:

The school must have in place an ICT policy covering the use of not only computers and network facilities, e-mail and Internet, but also any mobile technologies that the school chooses to use, including laptops, palmtops, personal digital assistants (PDAs), tablet PCs, USB pen drives and mobile phones.

Mobile phones and PDAs now have the potential to allow access to the Internet, affording instantaneous communication, offering the potential for collaboration, tutoring, research, communication and debate using native and foreign languages. Mobile phones and PDAs also have similar capabilities to e-mail in that they can be used to send and receive text and pictures. Schools should therefore consider the consequences of the misuse of all mobile technologies when drafting an ICT policy.

It is stressed that the Scottish Qualifications Authority prohibits taking mobile phones, WAP telephones or other electronic communications devices into examination rooms. There are also rules surrounding the use of calculators. Reference should be made to relevant SQA documentation.

Schools should also include in their ICT policy any communications applications they choose to employ, including video conferencing, digital imaging, web sites, discussion forums and video streaming.

Schools must ensure that all staff are aware of the content of the user policy Standard Circular 78, their responsibilities, and the consequences of misuse of the facility.

All school staff should be aware of the issues surrounding Internet access, e-mail and mobile technologies and the need for appropriate adult supervision.

The school should have a Responsible User Agreement for all pupils. Pupils under the age of eight years should not be expected to sign, but parents need to know what is expected of their children and to give permission for their children to use e-mail and the Internet by signing on their behalf. Pupils should be aware that all e-mail and Internet access is monitored.

Schools should inform parents/carers of children under 12 years of the use of computers, e-mail, all mobile technologies, the intranet and Internet and should give parents the opportunity to discuss/refuse their child's access according to their wishes and beliefs. It is strongly recommended that the school should take every opportunity to advise parents of all pupils of the conditions under which Internet access is granted.

Schools should also inform parents/carers of the use of digital photography and digital video and give parents the opportunity to discuss/refuse permission for their child to be photographed or to be part of a digital video recording according to their wishes and beliefs.

Schools should also inform parents/carers of the use of all mobile technologies. It is strongly recommended that the school should take every opportunity to advise parents of all pupils of the conditions under which the use of mobile phones is granted.

Relevant information for parents/carers is provided in Appendix 1. Schools are welcome to use this template or customise it to construct their own.

While "best of class" protection and filtering systems are in place, it is the nature of the Internet to be a dynamic and fast changing environment and it is not possible to give an absolute assurance that any pupil will never have access to inappropriate material. **There must be a written statement on how the school will respond in the event that pupils misuse the facility or in the event that inappropriate material is unavoidably displayed.**

Schools should ensure that Internet, e-mail and mobile technology safety issues are seen as an issue for teachers and staff across the curriculum and the whole school. Advice on the safe and responsible use of the Internet, e-mail and mobile technologies should be part of the Personal and Social Education/Personal and Social Development programme of study.

Every primary school has a copy of the Becta Internet Proficiency Scheme as recommended by the Scottish Executive and been advised of the websites which address the issues of Internet safety (Appendix 2).

7. The Role of the ICT Coordinator

Although a large amount of the network administration and maintenance has been centralised with the ERC ICT Network Team, there remain a number of functions which are required at school level. The Head Teacher of each school has the responsibility for overall use of the computer systems and school based servers in the school and in addition has responsibilities in the function and operation of the network. A nominated ICT coordinator, a designated senior member of staff, usually carries out this role.

The ICT coordinator is the key individual in all aspects of communication among the school, the ERC ICT Network Team, and the Education Department's ICT Central Technician Service. Both teams have set up on-line systems to aid communication. The activities expected of the ICT coordinator from the view of the support teams will include:

- ensuring that user lists are kept up to date;
- relaying account information and passwords to new users;
- advising support service of faults or support needs;
- discussing with support teams arrangements to deal with special occasions;
- advising support teams on suspected or actual misuse of systems or network facilities;
- taking suitable action when misuse of network systems is identified;
- ensuring that all users have completed a responsible user agreement;
- ensuring that staff are aware of Standard Circular 78 on use of ICT; and
- ensuring that school ICT policy relates to Education Department policies.

8. The Role of Parents or Carers

Parents have a responsibility to be aware that there may be risks associated with Internet, e-mail access and mobile technologies, and the steps the authority and the school is taking to address these. The school should ensure that parents are informed of the school's Acceptable Use Policy by issuing a copy of this document to parents.

Parents will also wish to ensure safe use in the home or in other contexts outwith school where a number of the above safety measures may be absent.

The Scottish Executive strongly recommends that parents refer to available advice about safe use of the Internet, e-mail and mobile technologies and ensure that they are aware of any access that is taking place. Guidance is available from a number of websites, listed in Appendix 2. Parents should also be aware that any evidence that pupils have been accessing material that should not be available through the school network will be considered seriously by educational and other professionals and may be dealt with formally.

9. Communication Applications

<u>E-mail</u>
Users should not disclose their password for access to the Education Network to anyone. No attempt should be made to access another user's account. Users must not send messages which are racist, sexist, which are threatening or contain offensive or obscene language. They must not send inappropriate sound or visual material. Users who receive inappropriate

messages or files should report this to the appropriate member of staff. Users should be aware that the authority logs all Internet and e-mail activity, and if requested, any individual's use of the Internet and e-mail can be provided.

School Web Sites

School web sites provide an interaction with pupils in school, pupils out of school, parents and the general public. It will be the responsibility of the school to provide and maintain this web-based information.

The use of images and information about children on schools websites is an issue for the reasons below:

- a child might be identified and targeted by an individual on the basis of material published online, placing the child at physical risk;
- a child's image might be stolen and manipulated by someone using imaging software to create offensive or illegal pornographic images; or
- another person may use the child's information to impersonate them.

Schools should therefore:

- not identify pupils by name or give e-mail addresses;
- avoid publication of photographs which ease image manipulation, particularly those pupils under 12 years of age;
- ensure a member of staff checks text written by pupils before publication, as it may contain potentially problematic materials such as personal information or libellous statements;
- ensure text does not include a pupil's full name;
- ensure a member of staff checks any additions to the school site before it goes live; and
- review any links placed on the site regularly.

Weblogs

The popularity of weblogs, or blogs, has grown in recent years. As with school websites, weblogs can provide pupils in school, pupils out of school, parents and the general public with information on particular subjects or themes. Weblogs also have the ability to provide the opportunity for direct involvement in their development via online posting and publishing of articles. It will be the responsibility of the school to provide and maintain this web-based information.

The issues on the use of images and information about children on weblogs are the same as those for school websites:

- a child might be identified and targeted by an individual on the basis of material published online, placing the child at physical risk;
- a child's image might be stolen and manipulated by someone using imaging software to create offensive or illegal pornographic images; or
- another person may use the child's information to impersonate them.

In addition, the communication that blogging facilitates must be closely monitored. Schools should therefore:

- moderate all posts and comments prior to publication via the setup process, ensuring that they are not racist, sexist, threatening, libellous or contain offensive or obscene language;

- ensure that pupils are not identified by their full name or e-mail address;
- ensure that users do not post personal information;
- avoid publication of close-up photographs of individual children; and
- regularly review any links placed on the weblog.

Video Conferencing

When using video conferencing, pupils should never give out personal information, including full names and contact details.

Online Discussion Forums

As with e-mail, users must not disclose their password for access to the discussion forum to anyone. They must not post messages which are racist, sexist, which are threatening or contain offensive or obscene language or content. For their own protection, they should not post personal information, disclosing telephone numbers or addresses.

10. Mobile Technologies

Appendix 3 comprises East Renfrewshire Education Department's document, *"The Use of Mobile Technologies within Educational Establishments".* This document states that mobile technologies provide powerful and exciting features and facilities which not only make a positive contribution to current lifestyles, but will also be used support learning and teaching. However, schools should consider the consequences of the misuse of mobile technologies when drafting an ICT policy.

Mobile Phones and Personal Digital Assistants (PDAs)

Mobile phones and PDAs now have similar capabilities to e-mail in that they can be used to send and receive text and pictures. As with e-mail, users must not send messages which are racist, sexist, which are threatening or contain offensive or obscene language or content. Users who receive inappropriate messages or files should report this to the appropriate member of staff. There is the possibility of recording sound and images which could intrude on the privacy of other people. Photographs of staff or pupils should therefore not be taken without permission, nor should images be used inappropriately. Equally, inappropriate content should not be downloaded from the Internet onto mobile phones, nor should inappropriate content be uploaded from mobile phones to systems connected to the Education Network.

Laptops, Palmtops and Tablet PCs

Laptops, Palmtops and Tablet PCs must not be connected to the network without prior permission.

Digital Cameras and Digital Video Cameras

Schools should inform parents/carers of the use of digital photography and digital video and give parents the opportunity to discuss/refuse permission for their child to be photographed or to be part of a digital video recording.

USB Drives

A USB drive, also known as a flash or pen drive, is a portable storage device used to transport files from one computer to another. Schools must alert staff, pupils, parents/carers that the responsibility for these devices and the security of the contents lies solely with the user and careful consideration should be given to the implications of the drive being misplaced, lost, stolen or damaged. It is strongly recommended, therefore, that staff and pupils store copies of

original files on USB drives, rather than the original files themselves and consciously reflect as to whether the stored information is of a confidential nature.

Schools must inform parents/carers of the anti-virus software installed on systems connected to the Education Network, stressing that updates to this software are downloaded on an hourly basis and when a user logs on to a workstation. Parents/carers should also be informed that all USB drives are immediately scanned for viruses on connection, further reducing any possibility of a USB drive inheriting a virus via connectivity to a workstation on the Education Network.

11. Conclusion

"The increase in the use of the Internet will continue to increase with the Scottish Government's Glow (formerly Scottish Schools' Digital Network (SSDN)) initiative which will complement the eventual roll-out of high-quality broadband connections across Scotland's schools.

Glow will create a national intranet for the education community including features which will enhance Internet safety. It will encourage online communication between schools and other participants in the education community and will be a catalyst for growing use of all aspects of ICT in schools. This increased use of ICT will bring significant benefits to learning and teaching.

The developments discussed in these guidelines which have all changed the nature and significance of the Internet and other electronic communications technologies have been addressed by implementing appropriate access and security policies and technical solutions at education authority and school level. Although Glow will assist in this regard through operating within a secure, managed environment, with built in safeguards for all users, there will remain an ongoing local requirement to manage services and the policies surrounding these, with a recognisable responsibility for authorities and schools to minimise risk."

DoubleClickThinking: Personal Safety on the Internet (2003)

These guidelines set out the relationship and responsibilities among East Renfrewshire Council's Education Department, the ERC ICT Network Team, the ICT Central Technician Service (Education) and individual education establishments.

The challenge is to ensure that all users and providers of the service are aware of their responsibilities, and are supported as required to carry out the duties associated with meeting these responsibilities.

John Wilson
Director of Education
August 2009

Appendix 1

Responsible User Agreement – Secondary Pupils

The use of computer equipment, education network and Internet is a privilege, not an automatic right. The computer equipment and the education network in the school are for use in connection with your school work and school activities. Access is given to a wide range of resources to assist your learning.

The authority logs all Internet and e-mail activity, and if requested, any individual's use of the Internet and e-mail can be provided to the school. The mail is not guaranteed to be private, and this logged record will be examined if it is thought that the system has been abused. Depending on the nature of the abuse, access to the network may be denied and you should be aware that further disciplinary action may be taken.

Security on computer systems and the network is extremely important. You should:

- Keep your username and password secure;
- Log off the network at the end of every session;
- Be careful not to give out any of your personal details or those of anyone you know when using the Internet, such as your name, address, phone number, e-mail address, picture or the name of the school;
- Immediately inform a member of staff if you are aware of a security problem;
- Ensure that settings and controls are not tampered with;
- Never attempt to log on using another person's account details;
- Never attempt to change, damage or destroy another person's data;
- Avoid introducing computer viruses onto the network by obtaining permission prior to using media brought from outwith the school.

Network Etiquette (Netiquette) principles should be used to ensure courtesy or politeness, and you are expected to abide by these principles. You should:

- Show fairness and consideration to other network users by ensuring messages sent are not threatening, rude or abusive, including the use of vulgar, racist or obscene language;
- Show respect for privacy and the rights of others by not sending inappropriate sound or visual material, including photographs and video.

When using the Internet you should:

- Log on at appropriate times;
- Search for and print information for school related activities only;
- Be careful not to access inappropriate websites;
- Leave a site immediately if inappropriate content is accidentally accessed and inform a member of staff;
- Ensure that downloaded material is not of an offensive or inappropriate nature;
- Be careful not to give out any of your personal details or those of anyone you know, such as your name, address, phone number, e-mail address, picture or the name of the school;
- Treat chat rooms with extreme caution due to their anonymous nature, and never attempt to meet anyone contacted through chat rooms. Immediately inform a member of staff if such a request is received;
- Be careful not to participate in any activity that may give offence to another person or organisation;
- Never use your access for commercial advertising;
- Seek permission to use copyrighted material.

When using e-mail you should:

- Only use the e-mail account provided by the school;
- Only use your own e-mail account;
- Ensure that messages and files sent are not threatening, racist, sexist, contain offensive or obscene language, pictures, photographs or video images;
- Inform a member of staff if you receive any messages or files that are of the above nature;
- Treat e-mails from unknown individuals with caution and never arrange to meet any person who contacts you through e-mail. Immediately inform a member of staff if such a request is received.

Mobile technologies include not only laptops, palmtops and tablet PCs but also mobile phones, Personal Digital Assistants (PDAs), cameras and USB drives. Mobile phones and PDAs have similar capabilities to e-mail in that they can be used to send and receive text and pictures and access the Internet. When using mobile technologies you should:

- Ensure that you have prior permission before connecting any mobile technologies to the network;
- Ensure that mobile technologies are not used during lessons/meetings or assemblies unless with the express permission of the class teacher. Any device which remains "on" during such times must be set to a silent mode;
- Ensure text messages sent are not threatening, rude or abusive, including the use of vulgar, racist or obscene language;
- Show respect for privacy and the rights of others by not sending inappropriate sound or visual material, including photographs and video;
- Store any received messages, sound or visual material that are of the above nature and immediately inform a member of staff, parent or carer;
- Be careful to whom you give your mobile phone number;
- Pass on another person's mobile phone number only if you have their permission to do so;
- Respect others' rights to privacy and only take photographs with their permission;
- Store copies of original files on USB drives, rather than the original files themselves;
- Carefully consider whether information stored on a USB drive is of a confidential nature;
- Ensure that stored, uploaded and downloaded material is not of an offensive or inappropriate nature.

You should note that the Scottish Qualifications Authority prohibits taking mobile phones, WAP telephones or other electronic communications devices into examination rooms. There are also rules surrounding the use of calculators, which your head teacher, subject teacher or SQA can provide advice.

If you agree to abide by the rules you may apply for access to the network by completing the contract below and requesting that your parent or carer also signs the contract.

Please return this section to the school.

Pupil Responsible User Agreement

I understand and will abide by the Responsible User Agreement. I understand that any violation of the regulations is unethical and may constitute a criminal offence. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken and/or any appropriate legal action.

I wish to apply for access to the East Renfrewshire Education Network.

School _____

Pupil _____

Signature _____ Date _____

Parent/Carer

As the parent or carer of this student, I have read the Responsible User Agreement. I understand that the access to the network is designed for educational purposes. I recognise that it is not possible to block access to all controversial materials and I will not hold the school or council responsible for materials accessed on the network. I hereby give permission for my child to have access to the educational network and internet.

Parent or Carer _____

Signature _____ Date _____

Responsible User Agreement – Primary Pupils

The computers and network, Internet access and e-mail available in school are for school work. There are rules about how these are to be used. You must keep to the rules or you will not be allowed to use the network.

- I will not pretend to be someone else when I am using the computer.
- I will be careful not to give out my name, address, phone number, e-mail address, picture or the name of the school when I am using the Internet or e-mail.
- I will be careful not to give out anyone else's name, address, phone number, e-mail address, picture or the name of the school when I am using the Internet or e-mail.
- I will not send nasty e-mails or e-mails which contain bad language.
- If I receive any e-mails that are nasty or have bad language I will tell my teacher straight away.
- I will not reply to e-mails from people I don't know.
- If anyone I don't know contacts me by e-mail, I will tell my teacher.
- I will never agree to meet anyone I don't know who contacts me by e-mail or on a mobile phone.
- I will only use the class e-mail address for school work.
- I will only use the Internet for school work.
- I will only print information for school work.
- I will take care of my own files and will not throw away or damage files that belong to someone else.
- I will not use my own USB drive or CDs without my teacher's permission.
- I will not use my mobile phone or camera without my teacher's permission.
- I will not take photographs or video without my teacher's permission.
- I will not send photographs or video without my teacher's permission.

To Parent or Carer

There is no doubt that Information and Communications Technology (ICT) can bring benefits to young people and enhance their learning experience. The vast array of information, often from the original source, and the instantaneous communication using a variety of media will change the way we experience life and work. It is essential that young people have the opportunity to experience these new technologies and to develop the searching, sorting and filtering skills that are likely to be part of their everyday life.

In our school most computers are connected to the school network and have access to the Internet. The use of computer equipment, education network and the Internet is a privilege, not an automatic right. The computer equipment and the education network in school are for use in connection with pupils' schoolwork and school activities. Access is given to a wide range of resources to assist their learning.

Your child will make supervised use of the World Wide Web and send and receive e-mails as part of their schoolwork. The Internet is a rich source of resources and a valuable place to look for information. The council has a single connection to the Internet for schools and maintains systems which prevent pupils having access to unsuitable material. It must be understood, however, that it is not possible to guarantee that pupils will not come across inappropriate material. The authority logs all Internet and e-mail activity, and if requested, any individual's use of the Internet and e-mail can be provided to the school. The mail is not guaranteed to be private, and this logged record will be examined if it is thought that the system has been abused. Depending on the nature of the abuse, access to the network may be denied and further disciplinary action may be taken.

We talk with pupils about using the network responsibly and how they should react to inappropriate material. We make sure that Internet access is supervised. It is important to teach pupils about the safe use of the computer systems and the network, network etiquette principles, the Internet and e-mail and the increasing use of mobile technologies. The following points are explained to the pupils:

Security on computer systems and the network is extremely important. Pupils should:

- Keep their username and password secure;
- Log off the network at the end of every session;
- Be careful not to give out any personal details or those of anyone they know when using the Internet, such as their name, address, phone number, e-mail address, picture or the name of the school;
- Immediately inform a member of staff if they are aware of a security problem;
- Ensure that settings and controls are not tampered with;
- Never attempt to log on using another person's account details;
- Never attempt to change, damage or destroy another person's data;
- Avoid introducing computer viruses onto the network by obtaining permission prior to using media brought from outwith the school.

Network Etiquette (Netiquette) principles should be used to ensure courtesy or politeness, and pupils are expected to abide by these principles. Pupils should:

- Show fairness and consideration to other network users by ensuring messages sent are not threatening, rude or abusive, including the use of vulgar, racist or obscene language; and

- Show respect to privacy and the rights of others by not sending inappropriate sound or visual material, including photographs and video.

When using the Internet pupils should:

- Log on at appropriate times;
- Search for and print information for school related activities only;
- Be careful not to access inappropriate websites;
- Leave a site immediately if inappropriate content is accidentally accessed and inform a member of staff;
- Ensure that downloaded material is not of an offensive or inappropriate nature;
- Be careful not to give out any of their personal details or those of anyone they know, such as their name, address, phone number, e-mail address, picture or the name of the school;
- Treat chat rooms with extreme caution due to their anonymous nature, and never attempt to meet anyone contacted through chat rooms. Immediately inform a member of staff if such a request is received;
- Be careful not to participate in any activity that may give offence to another person or organisation;
- Never use their access for commercial advertising;
- Seek permission to use copyrighted material.

When using e-mail pupils should:

- Only use the e-mail account provided by the school;
- Only use their own e-mail account;
- Ensure that messages and files sent are not threatening, racist, sexist, contain offensive or obscene language, pictures, photographs or video images;
- Inform a member of staff if they receive any messages or files that are of the above nature;
- Treat e-mails from unknown individuals with caution and never arrange to meet any person who contacts them through e-mail. Immediately inform a member of staff is such a request is received.

Mobile technologies include not only laptops, palmtops and tablet PCs but also mobile phones Personal Digital Assistants (PDAs), cameras and USB drives. Mobile phones and PDAs now have similar capabilities to e-mail in that they can be used to send and receive text and pictures and access the Internet. When using mobile technologies pupils should:

- Ensure that they have prior permission before connecting any mobile technologies to the network;
- Ensure that mobile technologies are not used during lessons/meetings or assemblies unless with the express permission of the class teacher. Any device which remains “on” during such times must be set to a silent mode;
- Ensure text messages sent are not threatening, rude or abusive, including the use of vulgar, racist or obscene language;
- Show respect for privacy and the rights of others by not sending inappropriate sound or visual material, including photographs and video;
- Store any received messages, sound or visual material that are of the above nature and immediately inform a member of staff, parent or carer;
- Be careful to whom they give their mobile phone number;
- Pass on another person’s mobile phone number only if you have their permission to do so;
- Respect others’ rights to privacy and only take photographs with their permission;
- Store copies of original files on USB drives, rather than the original files themselves;
- Carefully consider whether information stored on a USB drive is of a confidential nature;
- Ensure that stored, uploaded and downloaded material is not of an offensive or inappropriate nature.

You should note that the Scottish Qualifications Authority prohibits taking mobile phones, WAP telephones or other electronic communications devices into examination rooms. There are also rules surrounding the use of calculators, which your child's head teacher, subject teacher or SQA can provide advice.

Please return this section to the school.

School _____

Pupil _____

I agree/disagree that my child can have access to the Internet and email with the arrangements described above.

Signature of Pupil _____

Signature of Parent/Carer _____

Date _____

Appendix 2

Relevant Websites

For information:

East Renfrewshire Council	http://www.eastrenfrewshire.gov.uk
Double Click Thinking	http://www.ngflscotland.gov.uk/doubleclickthinking
Be Safe Online	http://www.besafeonline.org
Think U Know	http://www.thinkuknow.co.uk
Parents Online	http://www.parentsonline.gov.uk
Childnet International	http://www.childnet-int.org

For pupil use:

Think U Know	http://www.thinkuknow.co.uk
Kidsmart	http://www.kidsmart.org.uk
Chat Danger	http://www.chatdanger.com
Cyber Cafe	http://www.gridclub.com/have_a_go/ict/cybercafe/base.htm
For Kids by Kids Online	http://fkbko.co.uk
Know IT All	http://www.childnet-int.org/kia/

Appendix 3

East Renfrewshire Council: Education Department
The Use of Mobile Technologies within Educational Establishments

Purpose

This document seeks to provide guidance on the reasonable uses of mobile technologies on school premises and confirm support for and to head teachers in event that discipline is required to address behaviour by any person or persons making unacceptable use of these technologies. Because the technology changes so rapidly, it is pertinent to define these guidelines in general terms rather than specific in order to cover not only current technologies, but also future devices.

Background

In recent months, a range of powerful mobile technologies has become accessible to young people in our schools. These include cellular phones, photo-phones, video-phones, personal digital assistants (PDAs), laptop, palm or hand held computers, music storage and playback devices such as iPod, and video players now commonly in use by young people. Many of these devices are in use on school premises.

These technologies provide powerful and exciting features, many of which make a positive contribution to current lifestyles. Some of these features and facilities will be used to support teaching and learning, and for child safety reasons. The department is currently piloting systems which will improve communications with parents, by sending pre-recorded messages to mobile phones or answer phones. The vast majority of the use of these technologies is positive and integral to the lifestyle of most young people, although to some will appear trivial.

Regretfully, there is a growing portfolio of examples of issues arising from the inappropriate use of such devices and technologies by a minority. Some examples include: mobile phones ringing during lessons; young people “texting” during lessons; photo phones being used to take and send images inappropriately; using mobile phones and PDAs to connect to internet sites with inappropriate content; using mobile phones and PDAs to store unacceptable content, either pornographic, sectarian or racist; or bullying by text or phone.

It is the nature of this society that young people will acquire “the latest technology”. Further this group comprise the section of society most likely to exploit these technologies. There is a general ignorance among adults about the capabilities of young people with these devices.

Given the perceived benefits of these technologies and that the vast majority of users deploy them for their intended purpose, it is not appropriate to implement an outright and universal ban on such devices. Such action is likely to generate complaints from young people and parents who will reasonably quote child safety requirements in the case of mobile phones

The main aim should be to instigate a climate of personal responsibilities and respect for the rights of others to accompany the rights to access these technologies.

Everyone (staff, parents and young people) needs to be aware of the parameters of what is acceptable use of these devices within a school environment.

Policy

All schools must have a policy which defines for pupils, staff and parents what is acceptable, what is not, and the sanctions which will be applied if parameters are exceeded. This policy will be most effective if there is general agreement among young people, parents and staff as to its content, and that their views are represented during its drafting.

The policy should include:

Other than with the express permission of the class teacher, any communications device must not be used during lessons/meetings or assemblies. Any devices which remain "on" during such times must be set to a silent mode.

It is stressed that the Scottish Qualifications Authority prohibits taking mobile phones, WAP telephones or other electronic communications devices into examination rooms. There are also rules surrounding the use of calculators. Reference should be made to relevant SQA documentation.

To ensure the security of the education network, no mobile technologies, other than systems provided and installed by the education department, including laptop computers, may be connected to the education network by any means, cable, wireless, infra-red, Bluetooth or any similar technologies.

Schools must discuss with young people, the purpose and content of an agreement between each individual and the school about their rights and responsibilities in respect of mobile technologies. (It may be most convenient to append this to the responsible user agreement currently required before a pupil may connect to the education network.) An information sheet for parents should re-iterate the nature and purpose of the expanded responsible user agreement. Signed copies of the agreement, countersigned by the parent or carer, should be kept.

Parents and pupils must be aware of the hierarchy of sanctions which will apply if the mobile technologies are misused. Should it be deemed necessary to confiscate the device, then the pupil must be given the facility to make any reasonable call to a parent or carer.

In some situations the head teacher may request a meeting with a parent or carer before releasing the item.

The head teacher has the right to refuse any person, temporarily or permanently, the use of mobile technologies on school premises.

Head teachers have the right/responsibility to involve the police if criminal activity by any person is suspected.

John Wilson
Director of Education
August 2009