Revised Standard Circular 69 August 2020

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

EAST RENFREWSHIRE COUNCIL: EDUCATION DEPARTMENT

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

1. Introduction

"The internet and mobile technologies have positively transformed our lives, and those of children and young people. The internet provides children and young people with vast opportunities for learning, communication and support. It's becoming increasingly intertwined in their everyday lives with less distinction being made between the online and offline worlds. However, increasing reliance on online technologies makes us potentially vulnerable to those who seek to exploit these technological advancements for malicious purposes. We must all see the protection of children as our collective responsibility and we must all work together to ensure children and young people are protected online"

Internet Safety for Children and Young People: National Action Plan, Scottish Government, 2017

2. Background

The first UK Child Internet Safety Strategy was launched in December 2009. In April 2017, the Scottish Government launched the National Action Plan on Internet Safety for Children and Young People. This refreshed document was produced to ensure that we have appropriate frameworks of training, support and information in place for professionals and families, including children and young people and to help address some of the child Internet safety and responsible use issues in Scotland.

The following guidance draws together national recommendations, 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

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 make 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 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 ERC ICT Services.

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.

East Renfrewshire's Child Protection Committee has developed a section on East Renfrewshire Council's website, 'Online Safety for Children', to provide information on safety aspects of the Internet and practical tips and guidance for children, young people, parents and carers through links to external websites and useful documents.

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.

ERC ICT Services ensure that all systems connected to the Education Network have antivirus 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" (Revised August 2020)* 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. This also relates to any personally-owned devices connected to the Education Network.

East Renfrewshire Council's Education Department's Standard Circular 2, "Information Security within Educational Establishments" *(Revised August 2020)* outlines responsibilities in protecting all council information, especially any that has personal content, and guides staff to help ensure that all documentation is protected and handled appropriately in accordance with the Council's Charter for the Protection of Customer Information and the Information Security Statement of Intent.

5. The Role of ERC ICT Services

It is the role of ERC ICT Services to ensure that the security procedures in place for the Education Network conform to Council standards. The technological solutions used by ERC ICT Services 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, with appropriate password policy;

- 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 can be viewed by the ICT coordinator for information. As this method of access circumvents the normal filtering process the contents of these sites will be viewed by ERC ICT Services, 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. Any individual who considers that they have been subject to unacceptable behaviour is entitled to make a complaint. In serious circumstances ERC ICT Services reserves the right to suspend access to any user without prior consultation. The Head Teacher/ICT coordinator will be advised of such action immediately.

The Council's Information Security Officer has provided a range of advice and guidance on Information Security within the Information and Communications Technology (ICT) section of the Corporate Intranet.

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. 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.

Mobile technologies 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 technologies also have similar capabilities to e-mail in that they can be used to send and receive text, images, sound and video. 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 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, websites, 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.

Schools must ensure that all staff are aware of the content of Standard Circular 2 and their personal responsibilities in protecting all Council information, but especially any that has personal content.

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, email, 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 make parents/carers and learners aware of guidelines pertaining to live video conferencing.

Schools should also inform parents/carers of the use of digital photography and digital video which may be utilised on the school website, school social media accounts, school handbooks, publicity materials or on displays within the school 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. Curriculum for Excellence highlights through the experiences and outcomes the importance of Internet safety and responsible use:

Technologies - First and Second Levels

- I can extend my knowledge of how to use digital technology to communicate with others and I am aware of ways to keep safe and secure. TCH 1-03a
- I can explore online communities demonstrating an understanding of responsible digital behaviour and I'm aware of how to keep myself safe and secure. TCH 2-03a

Technologies - Third Level

- I can keep myself safe and secure in online environments and I am aware of the importance and consequences of doing this for myself and others. TCH 3-03a

Health and Wellbeing - Early to Fourth Levels

- I am learning to assess and manage risk, to protect myself and others, and to reduce the potential for harm when possible.
- I know and can demonstrate how to keep myself and others safe and how to respond in a range of emergency situations.

Child Internet safety and responsible use also refers to the education of children and young people to help them become more digitally literate.

Literacy - Second to Fourth Levels

- To help me develop an informed view, I can distinguish fact from opinion, and I am learning to recognise when my sources try to influence me and how useful these are. LIT 2-08a
- To help me develop an informed view, I am learning about the techniques used to influence opinion and how to assess the value of my sources, and I can recognise persuasion. LIT 3-08a
- To help me develop an informed view, I can identify some of the techniques used to influence or persuade and can assess the value of my sources. LIT 4-08a

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.

Advice on websites which address the issues of Internet safety are listed in Appendix 2.

7. The Role of the ICT Coordinator

Although a large amount of the network administration and maintenance has been centralised with ERC ICT Services, 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, and ERC ICT Services. Online systems have been put in place to aid communication. The activities expected of the ICT coordinator from the view of ERC ICT Services will include:

- ensuring that user lists are kept up to date;
- relaying account information and passwords to new users;
- advising ERC ICT Services of faults or support needs;
- discussing with ERC ICT Services arrangements to deal with special occasions;

- advising ERC ICT Services on suspected or actual misuse of systems or network facilities;
- taking suitable action when misuse of network systems is identified;
- ensuring that all pupils have completed a responsible user agreement;
- ensuring that staff are aware of Standard Circulars 69 and 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, email access and applications such as Google Classroom, Show my Homework etc, 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 Government states that, "The Internet is central to our everyday lives and those of our children. It can be a positive, fun place to interact with the world, with endless possibilities for learning and socialising. However, in enjoying the internet, we must also be aware that there are individuals and organisations that take advantage of the relative freedom the online environment provides, and that sadly, irresponsible and inappropriate use of the internet can often place children and young people at risk of harm."

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

E-mail

Users should not disclose their password for access to the Education Network to anyone. Users should adhere to the required password policy. 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 Websites

School websites 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 webbased information.

The use of images, video 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.

Blogs and School-Related Social Media

The popularity of blogs and school-related social media has grown in recent years. As with school websites, these can provide pupils in school, pupils out of school, parents and the general public with information on particular subjects or themes. They 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 Council's Social Media Policy provides clear guidelines to employees on the use of social media and a handbook for any staff members who manage their establishment's social media account.

The issues on the use of images and information about children on blogs or school-related social media 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 and posting comments 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 blog.

Video Conferencing

During times of remote or distance learning and teaching, schools will use Google Classroom, Google Meet and Microsoft Teams to keep in contact with learners and hold online learning. This may involve the use of video conferencing, video lessons and live lessons. Schools must ensure that pupils adhere to the following guidelines:

- Be aware of their surroundings and background
- If using video, check lighting and the quality of sound from their microphone
- Be aware of and limit any noise in their environment – e.g. pets, domestic appliances
- If pupils have one available, they should use a headset rather than the microphone built-in to their device
- Check what is visible on screen and 'blur' their background
- If using a laptop, consider raising it so that pupils are looking directly into the screen

- Log on to live lessons from a suitable location in their home. This should not be their bedroom.
- Pupils must dress appropriately at all times
- Pupils should consider who else might be able to hear what they are saying and see them on screen
- Pupils should not record or take photographs during the live lesson
- Pupils should maintain standards of behaviour.

Due to the timing of certain vocational or instrumental music courses, it may be necessary for some pupils to access online/live video lessons from within the school building. On these occasions, pupils would be expected to adhere to the same guidelines set out above, as applicable.

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
Mobile phones have similar capabilities to e-mail in that they can be used to send and receive text, images, sound and video. 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, sound recordings or video footage 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.

School Owned Mobile Technologies
School owned "managed devices" are those which allow staff and pupils to log on in a similar way to those wired to the Education Network. They allow access to Home Folders, shared drives, e-mail and filtered Internet access.

All other school owned mobile technologies are "unmanaged" and as such must not be connected to the Education Network without prior permission. Such devices will not be able to access Home Folders and shared drives.

Personally Owned Devices
All educational establishments have wireless access meaning that you may connect personally owned devices to ERC's Education Network to support learning and teaching in accordance with Standard Circular 78.

Schools are encouraged to responsibly promote 'Bring your own Technology/Device' (BYOT/D) approaches. On a personally owned device, use of 3G or 4G service will not provide the safety benefits of ERC's Education Network's filtered Internet access. Use of a 3G or 4G service may also cost the owner money.

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. This is a legal obligation under the Data Protection Act.

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.

Staff, on connecting an unencrypted USB drive to any system on the Education Network will be prompted to encrypt the device. Standard Circular 2 states that it is against Council policy to hold **OFFICIAL SENSITIVE** data on a personal owned computing device. Any document which is marked **OFFICIAL SENSITIVE** whether electronic or paper based, and relates to child protection or criminal activity, should not be taken out of school, without management approval. This applies even when such documents are stored on an encrypted USB pen drive

Guidelines on dealing with a loss of information, laptop or USB drive are available under Information Security within the ICT section of the Corporate Intranet.

11. Conclusion

"Scotland's Digital Strategy, published in March 2017, features actions on improving digital connectivity, supporting our digital industries, building digital public services, expanding our pool of digital skills, ensuring we are a cyber-resilient and secure nation, and ensuring everybody can share in the social, economic and democratic opportunities of digital. It also recognises the challenges that digital poses for work, society, and our economy; and that collective action will be needed to ensure nobody is left behind"

National Action Plan on Internet Safety for Children and Young People, Scottish Government. 2017

Glow is a national intranet for the education community including features which enhances Internet safety. It encourages online communication between schools and other participants in the education community and is a catalyst for growing use of all aspects of ICT in schools. Through Glow there are a variety of productivity tools available for users, this increased use of ICT has brought 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.

These guidelines set out the relationship and responsibilities among East Renfrewshire Council's Education Department, ERC ICT Services 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.

Mhairi Shaw
Director of Education
August 2020

Appendix 1

Digital Responsible User Agreement

- Digital devices (like desktop computers, laptops, Chromebooks and iPads), internet access and email available in school are for school work only.
- These rules show you how you should use these in school.
- You must keep to the rules or you will not be allowed to use a desktop computer, laptop, Chromebook or an iPad in school.

Ask your teacher before you use a digital device like a desktop computer, laptop, a Chromebook or an iPad

Always write happy and polite messages, and only to people you know

Keep your name, your address, your school and your pictures top secret

Keep your passwords safe, and try to remember them in your head

Tell your teacher or another adult if you see something on a device that you don't like

Ask your teacher or another adult before you take pictures or make videos

Parent/Carer signature:

Child's signature:

Responsible User Agreement – Primary Pupils

The digital devices and network, Internet access and email 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.

Do not pretend to be someone else when you are using the computer.
Do not give out your name, address, phone number, email address, picture or the name of your school when using the Internet or email
Do not give out anyone else's name, address, phone number, email address, picture or the name of your school when using the Internet or email
Do not send nasty emails or emails which contain bad language.
If you receive any emails that are nasty or have bad language, tell your teacher straight away.
Do not reply to emails from people you do not know.
If anyone you do not know contacts you by email, tell your teacher.
Never agree to meet anyone you do not know who contacts you by email or on a mobile phone.
Only use the class email address and your Glow email address for school work.
Only use the Internet for school work.
Only print information for school work.
Take care of your own files and do not throw away or damage files that belong to someone else.
Do not use your own USB drive without your teacher's permission.
Do not use your mobile phone or camera without your teacher's permission.
Do not take photographs or record voice or video without your teacher's permission.
Do not send photographs, sound or video without your teacher's permission.
Only connect your own device to the wireless network when you have approval and asked to use your device for school work.
When using Google Meet or Microsoft Teams for a video lesson, behave as you are expected to in a real classroom during a face-to-face lesson.
Make sure your microphone is on mute, unless you would like to speak.
Make sure that you choose an appropriate place to join the video lesson and that no personal items can be seen by others.

Letter to Parent/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 digital devices are connected to the school network and have access to the Internet. The use of digital devices, the Education Network and the Internet is a privilege, not an automatic right. The digital 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 Internet and send and receive emails 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 email activity, and if requested, any individual's use of the Internet and email 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 misused. Depending on the nature of the misuse, access to the network may be denied and further disciplinary action may be taken. This applies to the misuse of any resources using a personally owned device.

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 email 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, email 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, email 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;
- Ensure copyright free material is used whenever possible and if necessary seek permission to use copyrighted material.

When using email pupils should:

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

Mobile technologies include, but are not limited to: laptops, tablet devices, phones, cameras, virtual reality headsets and USB drives. When using mobile technologies pupils should:

- Ensure that they have prior permission before connecting any mobile technologies to a device on 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, record voice and video footage 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.

As all educational establishments have wireless access, pupils may connect personally owned devices to ERC's Education Network to support their learning. Schools should encourage approaches to 'Bring Your Own Technology/Device' (BYOT/D). When personally owned devices are being used for school work, they should be connected to the wireless network, this will ensure that pupils benefit from firewall and filtering settings. Using personally owned devices with 3G or 4G service will not provide the safety benefits of ERC's Education Networks' filtered Internet access and may cost money.

During times of remote or distance learning and teaching, schools will use Google Classroom, Google Meet and Microsoft Teams to enable learning with pupils and keep in contact with classes. This may involve the use of video conferencing, video lessons and live lessons. Due to the timing of instrumental music lessons, it may be necessary for some pupils to access online/live video lessons from within the school building.
On these occasions, pupils would be expected to adhere to the same guidelines set out below, as applicable.

Pupils should:

- Be aware of and limit any background noise – e.g. pets, tv, radio etc
- Behave as they are expected to in a real classroom during face-to-face lessons.
- Sit with their backs to a wall and try not to have personal items on display that could be seen by others. If using Teams, pupils should blur their background.
- Log on to live lessons in an appropriate space at home but not from their bedroom.
- Dress appropriately.
- Consider who else might be able to hear what they are saying and see them on screen
- Not record or take photographs during the live lesson
- (If using a laptop) consider raising it so that they are looking directly into the screen
- Follow all guidance and instructions from their teacher during the lesson
- Leave the video lesson when asked to do so by their teacher.
- Contact their teacher if there was anything during an online lesson that concerned them, as they usually would in school.

Please return this section to the school.

Pupil Responsible User Agreement - Primary

The information you supply on this form will be used by East Renfrewshire Council as pupil administrative information. We will use your information to verify your identity where required, contact you by post, email, text message or telephone and to maintain our records. The council will use this information because we need to do so to perform a task carried out in the public interest. The information will be shared with SEEMiS, CRB, ParentPay, the Diocese of Paisley (in Roman Catholic schools), Scottish Government including their Analytical Services, Education Scotland, Glow (Scotland's national education network), SQA, 2Cqr, ESgoil, BAM FM (Carlibar Primary, Barrhead Mearns Castle, Williamwood, Woodfarm High Schools), Bellrock FM (Mearns Primary and St Ninian's High), Skills Development Scotland, Scholar (Heriot Watt University) and East Renfrewshire Culture and Leisure Trust to provide this service and to protect public funds by preventing fraud. If you do not provide us with the information we have asked for then we will not be able to provide this service to you. We also need to process more sensitive personal information about you for reasons of substantial public interest as set out in the Data Protection Act 2018. It is necessary for us to process it to carry out key functions as outlined in law. If you do not have access to a digital device and wish a paper copy please let us know by contacting your child's school. If you have provided anyone else's details on this form, please make sure that you have told them that you have given their information to East Renfrewshire Council. We will only use this information in the event of an emergency. If you or they want any more information on how we will be using and handling this information, visit our web site at www.eastrenfrewshire.gov.uk/privacy.

School ______________________________

Pupil ______________________________

Please tick as appropriate

	Agree	Disagree
I would like my child to have access to the Education Network, Internet and e-mail with the arrangements described above.		

School ______________________________

Pupil ______________________________

Signature of Pupil ______________________________

Signature of Parent/Carer ______________________________

Date ______________________________

Responsible User Agreement – Secondary Pupils

The use of digital devices, the Education Network and the Internet is a privilege, not an automatic right. The digital devices 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 with your learning.

The authority logs all Internet and email activity, and if requested, any individual's use of the Internet and email can be provided to the school. The email is not guaranteed to be private, and this logged record will be examined if it is thought that the system has been misused. Depending on the nature of the misuse, access to the network may be denied and you should be aware that further disciplinary action may be taken. This applies to the misuse of any resources using a personally owned device.

Security on digital devices 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, email 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, email 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;

- Ensure copyright free material is used whenever possible and if necessary, seek permission to use copyrighted material.

When using email you should:

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

Mobile technologies include but are not limited to laptops, tablet devices, phones, cameras, virtual reality headsets and USB drives. When using mobile technologies you should:

- Ensure that you have prior permission before connecting any mobile technologies to a device on 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, record voice and video footage 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.

As all educational establishments have wireless access, pupils may connect personally owned devices to ERC's Education Network to support their learning. Schools should encourage approaches to 'Bring Your Own Technology/Device' (BYOT/D). When personally owned devices are being used for school work, they should be connected to the wireless network, this will ensure that pupils benefit from firewall and filtering settings. Using personally owned devices with 3G or 4G service will not provide the safety benefits of ERC's Education Networks' filtered Internet access and may cost money.

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

Due to the timing of certain vocational courses, it may be necessary for some pupils to access online/live video lessons from within the school building. On these occasions, pupils would be expected to adhere to the same guidelines set out below, as applicable.

During times of remote or distance learning and teaching, your school will use Google Classroom, Google Meet and Microsoft Teams to keep in contact with you and hold online learning. This may involve the use of video conferencing, video lessons and live lessons.

- Be aware of your surroundings and your background
- If using video, check your lighting and the quality of sound from your microphone
- Be aware of and limit any noise in your environment – e.g. pets, domestic appliances
- If you have one, use a headset rather than the microphone built-in to your device
- Check what is visible on screen and 'blur' your background
- If using a laptop, consider raising it so that you are looking directly into the screen
- Don't log on to live lessons from your bedroom
- Dress appropriately at all times
- Consider who else might be able to hear what you are saying and see you on screen
- Do not record or take photographs during the live lesson
- Maintain standards of behaviour.

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 – Secondary

The information you supply on this form will be used by East Renfrewshire Council as pupil administrative information. We will use your information to verify your identity where required, contact you by post, email, text message or telephone and to maintain our records. The council will use this information because we need to do so to perform a task carried out in the public interest. The information will be shared with SEEMiS, CRB, ParentPay, the Diocese of Paisley (in Roman Catholic schools), Scottish Government including their Analytical Services, Education Scotland, Glow (Scotland's national education network), SQA, 2Cqr, ESgoil, BAM FM (Carlibar Primary, Barrhead Mearns Castle, Williamwood, Woodfarm High Schools), Bellrock FM (Mearns Primary and St Ninian's High), Skills Development Scotland, Scholar (Heriot Watt University) and East Renfrewshire Culture and Leisure Trust to provide this service and to protect public funds by preventing fraud. If you do not provide us with the information we have asked for then we will not be able to provide this service to you. We also need to process more sensitive personal information about you for reasons of substantial public interest as set out in the Data Protection Act 2018. It is necessary for us to process it to carry out key functions as outlined in law. If you do not have access to a digital device and wish a paper copy please let us know by contacting your child's school. If you have provided anyone else's details on this form, please make sure that you have told them that you have given their information to East Renfrewshire Council. We will only use this information in the event of an emergency. If you or they want any more information on how we will be using and handling this information, visit our web site at www.eastrenfrewshire.gov.uk/privacy.

To be completed by Pupil:	Agree	Disagree
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 East Renfrewshire's Education Network, Internet and email.		

School ______________________________

Pupil ______________________________

Signature ____________________ Date ____________

To be completed by Parent/Carer:	Agree	Disagree
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.		
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 Education Network, Internet and email.		

Parent or Carer ______________________________

Signature ____________________ Date ____________

Appendix 2

Relevant Websites

Think U Know	http://www.thinkuknow.co.uk
Respect Me	http://www.respectme.org.uk/
Chat Danger	http://www.chatdanger.com
Kidsmart	http://www.kidsmart.org.uk
Get Safe Online	http://www.getsafeonline.org/
Be Safe Online	http://www.besafeonline.org
Digizen	http://www.digizen.org/
Childnet International	http://www.childnet-int.org
Have Fun – Stay Safe	http://www.havefunstaysafe.info/cms/
Cyber Cafe	http://www.thinkuknow.co.uk/8_10/cybercafe/Cyber-Cafe-Base/
Know IT All	http://www.childnet-int.org/kia/
ERC Child Protection Information about Community and Online Safety	https://www.eastrenfrewshire.gov.uk/online-safety-for-children

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

A range of powerful mobile technologies has become accessible to 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 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; devices being used to take and send images inappropriately; using mobile technologies to connect to Internet sites with inappropriate content; using mobile technologies 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 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 "managed devices", may be connected without prior permission.

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.

Mhairi Shaw
Director of Education
August 2020