Roe Valley Integrated Primary School

E-safety, ICT Acceptable Use and Digital Media Policy

Signature of Chair of Board of Governors: _____Ratified: _____

Signature of Principal: _____

Signature of ICT Coordinator _____

Reviewed and updated: December 2017

Review due: December 2018

Background

This policy applies to all the members of the Roe Valley Integrated Primary School community (staff, pupils, volunteers, parents/guardians, visitors and community users) who have access to and are users of school ICT resources and software both in and outside of the school.

This document sets out the policy and practices for the safe and effective use of the Internet in Roe Valley Integrated Primary School. The policy has been drawn up by the staff of the school under the leadership of Mrs J McDonagh, Principal and Miss J Holmes, ICT coordinator. It has been approved by the Board of Governors and is available to all parents via the school office if requested.

The policy and its implementation will be reviewed annually.

What is E-safety?

E-safety is short for electronic safety. It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. E-safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The school requires that pupils/parents sign the user agreement documents as a means of demonstrating that the policy has been communicated to all users throughout the school. It includes doing anything outside of school and/or online, that may bring the school's name into disrepute. This will include posting derogatory information about teachers or the school **(see policy on Parental Use of Social Networking and Internet Sites).**

Internet Safety Policy

The Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. Roe Valley IPS provides pupils with opportunities to use the excellent resources available on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

C2K

Classroom 2000 (C2k) is the project responsible for the provision of information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

Some of these safety services include:

- Providing all users with a unique user name and password
- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses
- Filters access to web sites
- Providing appropriate curriculum software.

Should the school decide to access online services through service providers other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. We have a Code of Safe Practice for pupils and staff containing E-Safety Rules which makes explicit to all users what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones and camera phones) is subject to the same requirements as technology provided by the school.

Miss J Holmes, the ICT Co-ordinator and Mrs J McDonagh, the Principal will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Safe Practice for Pupils

A parental/carer consent letter accompanied by the code of practice for pupils is sent out annually to parents/carers and this consent must be obtained before the pupil accesses the Internet.

In addition, the following key measures have been adopted by Roe Valley Integrated Primary School to ensure our pupils do not access any inappropriate material:

- The school's E-Safety code of practice for Use of the Internet and other digital technologies is made explicit to all pupils and E-Safety guidelines are displayed prominently throughout the school
- Our Code of Practice is reviewed each school year and signed by pupils/parents
- Pupils using the Internet will normally be working in highly-visible areas of the school and monitored where possible by the teacher/classroom assistant
- All online activity is for appropriate educational purposes and is supervised, where possible
- Pupils will, where possible, use sites pre-selected by the teacher and appropriate to their age group
- Pupils in Key Stage 2 are educated in the safe and effective use of the Internet, through a number of selected websites, e-safety workshops, assemblies and Safer Internet day

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

The use of mobile phones by pupils is not permitted on the school premises during school hours. During school hours' pupils are forbidden to play computer games or access social networking sites.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school's Discipline/Behaviour Policy. Minor incidents will be dealt with by Mrs J McDonagh, Principal and may result in a temporary or permanent ban on Internet use. Incidents involving child protection issues will be dealt with in accordance with the school's child protection policy and reported to the school CEOP ambassador, Miss J. Holmes.

Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff:

- Pupils accessing the Internet should be supervised by an adult at all times
- Staff will make pupils aware of the rules for the safe and effective use of the Internet. These are displayed in classrooms and discussed with pupils
- All pupils using the Internet have written permission from their parents
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinator/CEOP ambassador
- In the interests of system security staff passwords should only be shared with the network manager (Miss J. Holmes)
- Teachers are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these
- Photographs of pupils should, where possible, be taken with a school camera and images should be stored on a centralised area on the school network, accessible only to teaching staff or under supervision for pupil work
- School systems may not be used for unauthorised commercial transactions

Internet Safety Awareness

In Roe Valley Integrated Primary School we believe that, alongside having a written E-Safety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Internet Safety Awareness for pupils

- Rules for the Acceptable Use of the Internet are discussed with all pupils and are prominently displayed in classrooms. In addition, Key Stage 2 pupils are made aware and discuss Internet Safety through structured lessons, workshops and Safer Internet Day. There are various pupil resources available.

Internet Safety Awareness for staff

- The ICT Co-ordinator keeps staff informed and updated on issues relating to Internet Safety. All teaching staff, classroom assistants and supervisory assistants are in turn made aware of the Departments policy and strategy on ICT use in teaching and learning and updated in relation to relevant changes.

- **The Child Exploitation and Online Protection Centre (CEOP)** runs regular one-day courses for teachers in Northern Ireland. These are advertised directly to schools. Teachers can download lesson plans, teaching activities and pupils' worksheets by registering with the Thinkuknow website. CEOP ambassador within the school is Miss J. Holmes.

Internet Safety Awareness for parents

- **The Internet Safety Policy and Code of safe Practice for pupils is sent home at the start of each school year for parental signature. Additional advice for parents with internet access at home also accompanies this letter or Internet safety leaflets for parents and carers also are sent home annually. Parents/carers are also invited bi-annually to attend an E-safety workshop.**

Health and Safety

In Roe Valley Integrated Primary School we have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources. Pupils are supervised at all times when using Interactive Whiteboards and Digital Projectors are being used. Guidance is also issued to pupils in relation to the safe use of computers, interactive whiteboard and projectors. Such guidance includes advice concerning correct posture, positioning of screens, ensuring pupils do not stare directly into the beam of a projector etc.

Wireless Networks

The Health Protection Agency has advised that there is no consistent evidence of health effects from radio frequency exposures below guideline levels and therefore no reason why schools and others should not use WiFi (Wireless Fidelity) equipment. Further information on WiFi equipment is available at: the Health Protection Agency website.

School Website

The school web site is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the website reflects the school's ethos that information is accurate and well-presented and that personal security is not compromised. An editorial team ensure common values and quality control. As the school's website can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply.

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Social Software

- This is a generic term for community networks, chatrooms, instant messenger systems, online journals, social networks and blogs (personal web journals). Social environments enable any community to share resources and ideas amongst users. Such software allows users to exchange resources, ideas, pictures and video.

- The majority of activity in these on-line social sites usually causes no concern. C2k filters out these social networking sites and blocks attempts to circumvent their filters leaving it

relatively safe in the school environment. Concerns in relation to inappropriate activities would tend to come from use outside the school environment.

- We regard the education of pupils on the safe and responsible use of social software as vitally important and this is addressed through our Internet Safety Education for pupils.

- Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school's discipline policy and child protection procedures.

- Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

- The school will take very seriously any behaviour by a pupil or parent online that could bring the school's name into disrepute. This will include any derogatory information or postings about staff or pupils. The school will not hesitate to involve outside agencies such as PSNI or to seek legal advice on such matters.

Roles and Responsibilities

The E-safety roles and responsibilities of individuals and groups within Roe Valley Integrated P.S are as follows-

Governors

- The Board of Governors is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Principal

- The Principal has a duty of care for ensuring the safety (including E-safety) of members of the school community, though the day to day responsibility for E-safety will be delegated to the ICT Co-ordinator (Miss J. Holmes)
- The Principal should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Principal is responsible for ensuring that the ICT Co-ordinator and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

ICT Co-ordinator

- The ICT Co-ordinator leads the pupils and staff, and has a leading role in establishing and reviewing the school E-safety policies along with the Principal and appropriate pastoral staff.
- The ICT Co-ordinator ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place, provides training and advice for staff, liaises with school technical staff and receives reports of E-safety incidents and, if necessary, creates a log of incidents to inform future E-safety developments.
- The ICT Co-ordinator is, along with the Designated Teacher for Child Protection, the first point of contact for all E-Safety issues. She will immediately liaise with the Designated Teacher or Deputy Designated Teacher or other senior members of staff.
- The provision of the ICT managed service is delivered by C2k. It is the responsibility of the ICT Co-ordinator to ensure that the managed service provider carries out all the relevant safety measures and that any breaches of the safety measures are reported to the C2k Service Help Desk and the E-safety Co-ordinator.

Teaching staff

Staff are responsible for:

- Ensuring that they have an up to date awareness of e-safety matters and of the E-safety Policy and practices (they have read, understood and signed the Acceptable Use Policy)
- Reporting any suspected misuse or problem to the ICT Network Manager and the Designated Teacher for Child Protection in the first instance, or the Deputy Designated Teacher or other senior members of staff in his/her absence, ensuring that all digital communications with pupils/parents/guardians are on a professional level and only carried out using official school systems
- Ensuring that E-safety issues are embedded in all aspects of the curriculum and other activities
- Ensuring pupils understand and follow the E-safety and acceptable use policies when using ICT equipment within their subject area or pastorally
- Ensuring pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Monitoring the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implementing current policies with regard to these devices

- In lessons where internet use is pre-planned, guiding pupils to sites checked as suitable for their use and making sure that processes are in place for dealing with any unsuitable material that is found in internet searches
- Immediately advising the ICT Co-ordinator (or, in her absence, a member of the Senior Management Team) in the event of any issues of concern relating to E-safety matters

Whilst access to the internet on the C2k and non-C2K systems is heavily filtered to protect the interests of staff and pupils, in certain circumstances access may be granted to staff to sites which would normally be restricted. Requests for access to blocked sites should be made to the ICT Co-ordinator. In accessing these sites, staff should exercise caution. These sites may contain inappropriate or questionable information, including user generated content. It is the responsibility of staff who wish to use these restricted sites to vet the links they plan to use.

Particular care should also be taken while projecting information from a digital media device onto a whiteboard or other form of facility, as inappropriate material may be displayed.

Any resources or materials downloaded by staff, pupils or parents for use within school, must be in line with the requirements of this policy and be suitable for use in the classroom. If an individual is unsure regarding the appropriateness of content, he/she should seek advice from the ICT Co-ordinator before accessing the material within school (or in her absence, another member of the Senior Management Team).

All school resources (including computers, laptops, tablets and other digital devices) and their associated accessories are provided for educational use; they must not be used for any other purposes. Only portable resources may be removed from school when the 'Staff Loan of School Equipment Agreement' has been signed and returned, to facilitate preparation for teaching and learning.

Staff will be made aware that the school's filtered internet and e-mail services are monitored and are not therefore private – internet activity and e-mail messages can be viewed by the Principal at any time. While normal privacy is respected and protected by password controls, users must not expect internet, e-mail or files to be absolutely private. Accounts can be disabled and passwords changed when deemed appropriate or necessary.

Pupils – Digital Leaders

The internet and digital media are provided for pupils to conduct research, communicate with others and fulfil their curricular requirements. While the use of ICT is a required aspect of the statutory Northern Ireland Curriculum, access to the internet, digital media and C2k NI services remains a privilege and not a right. Access to the internet and digital media requires

parental permission and a signed declaration by pupils agreeing to the school rules for the use of the internet and digital media. Access is granted to pupils who act in a considerate and responsible manner, and will be withdrawn if they fail to maintain acceptable standards of use.

Pupils are responsible for:

- Good behaviour when using the internet and digital media just as they are in the classroom or elsewhere in the school
- Complying with all copyright, libel, fraud, discrimination and obscenity laws when using the internet and digital media at school
- Advising their teacher immediately if at any time pupils find themselves able to access, from within the school system, internet sites which they think should be blocked
- Using the school digital media in accordance with the Pupil Acceptable Use Policy
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to do so
- Understanding policies on the use of mobile devices and digital cameras and on the taking / use of images and on cyber-bullying
- Understanding the importance of adopting good E-safety practice when using digital technologies out of school and acknowledging that the school's E-safety Policy covers their actions out of school, if related to their membership of the school

Pupils will be made aware that the school's filtered internet and e-mail services are monitored and are not therefore private – internet and e-mail messages can be viewed by the Principal at any time. While normal privacy is respected and protected by password controls, users must not expect internet and cloud activity, e-mail or files to be absolutely private. Accounts can be disabled and passwords changed when deemed appropriate or necessary.

As a representative of the school, each pupil will accept responsibility for reporting any misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any material sent or received that indicates or suggests pornography, unethical or illegal requests, racism, sexism, homophobia, inappropriate language or any use which may be likely to cause offence and other issues.

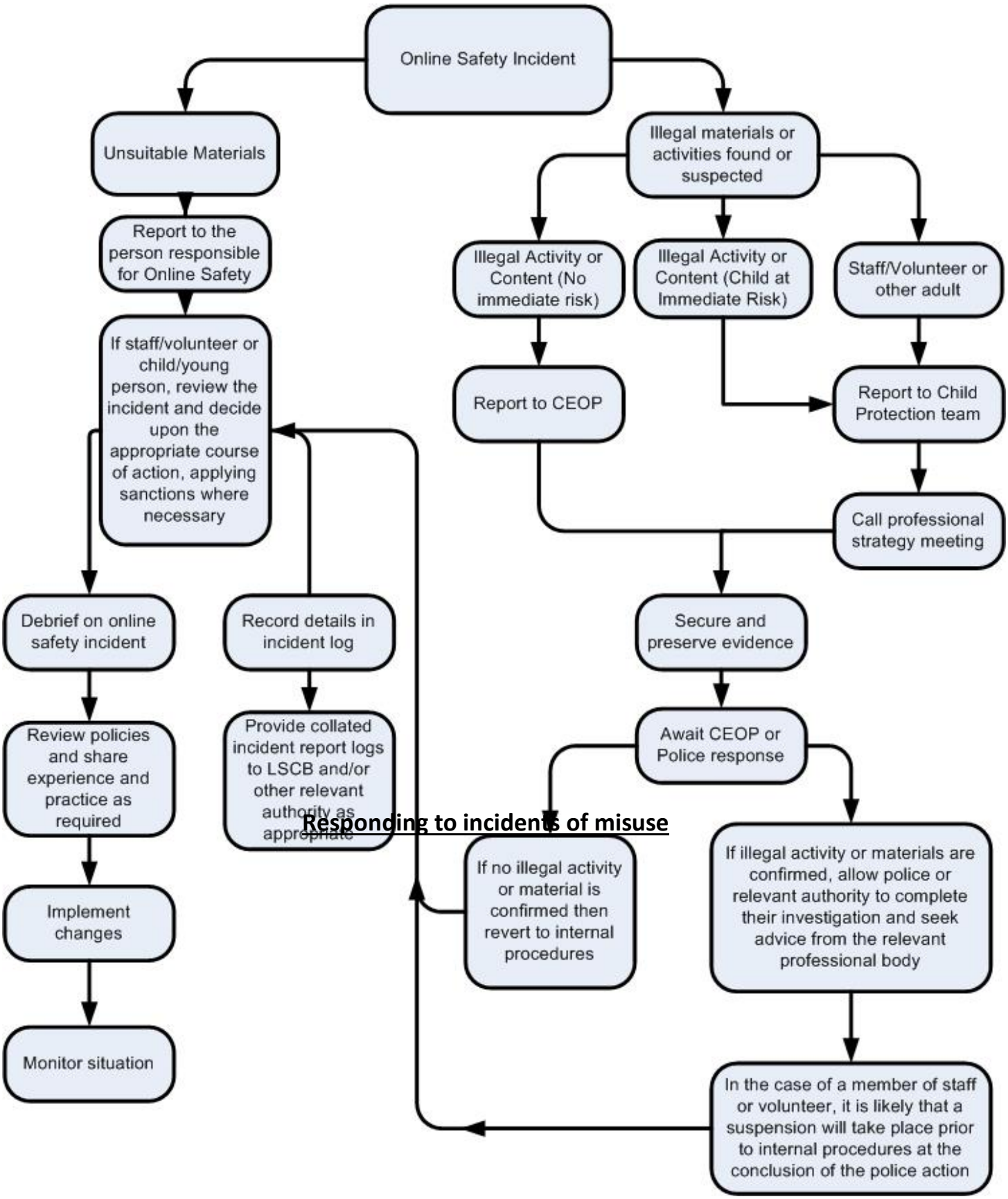
Designated and Deputy Designated Teacher for Child Protection

The Designated and Deputy Designated Teacher for Child Protection will be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues arising from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

If the DT and/or DDT are made aware of pupils accessing/playing online/console games containing inappropriate content and/or which are not age appropriate the school will record this information and may contact you. **This may be addressed as a child protection e safety issue.**

Responding to incidents of misuse -overleaf



Responding to incidents of misuse

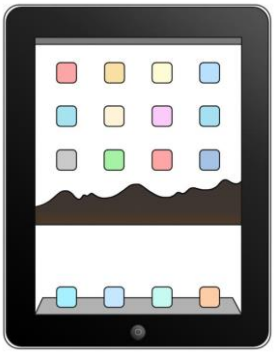
ICT Code of Safe Practice

E-Safety Rules for Pupils

- I will only use ICT in school for school purposes
- I will only use my class e-mail address or my own school e-mail address when e-mailing

- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-safety.



Signed _____ (child /or parent of young child)

Name of Child _____ Class _____

ICT Code of Safe Practice for Staff

E-Safety Rules

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to

this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with Miss J. Holmes (school E-safety coordinator) or Mrs J. McDonagh (Principal)

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, C2k, secure e-mail system for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of Miss J. Holmes
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request to the Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school

Signature …………………………………………. Date ……………………

Full Name …………………………………….... (Printed)

Job Title ………………………………………………………………………………

Parental Agreement/Consent Letter

Dear Parent/ Carer,

As part of Roe Valley Integrated Primary School's Information and Communications Technology programme, we offer pupils supervised access to a *filtered* Internet service

provided by C2k. Access to the Internet will enable pupils to explore and make appropriate use of many web sites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However in spite of the tremendous learning potential, you should be advised that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service provider C2k has installed filtering software which operates by blocking thousands of inappropriate web sites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter. Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs J.McDonagh

✂----------

Parent/ carer signature

We have discussed this and

…….... (Child name) agrees to follow the E-safety rules and to support the safe use of ICT at Roe Valley Integrated Primary School

Parent/ Carer Signature ……

Date ……

Additional Advice for Parents with Internet Access at home

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.

2. Parents should agree with their children suitable days/times for accessing the Internet.

3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use;

4. Parents should get to know the sites their children visit and talk to them about what they are learning;

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below);

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;

7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school they should immediately inform the school.

9. It should be noted that the school will take very seriously any behaviour by a pupil or parent online that could bring the school's name into disrepute. This will include any derogatory information or postings about staff or pupils. The school will not hesitate to involve outside agencies such as PSNI or to seek legal advice on such matters.

Further advice for parents is available from the following sources:

-

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.

- http://www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
- http://www.bbc.co.uk/webwise Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.
- http://www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.
- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)
- http://www.parents.vodafone.com Vodafone's site is designed to help

Seesaw – Parental information and acceptance

Dear Parents:

I am delighted to share with you that this school year, our class will be using Seesaw (http://seesaw.me), a secure online journal where students can document what they are learning in class. Your child will be able to add the things we work on (including photos, videos, worksheets, drawings and voice recordings) to their Seesaw journal and we can share them privately with you and other family members to view and comment on.

In order for your child to use Seesaw, certain personally identifiable information – like the student's name, photos, videos or voice recordings – may be collected. Seesaw has a robust privacy policy (https://app.seesaw.me/about/privacy) and is committed to never share or sell your child's personal information or journal content.

Under a federal law titled the Children's Online Privacy Protection Act (COPPA), in order for your child to use Seesaw, we must provide you with notification and obtain your permission. For more information on COPPA, please visit https://www.ftc.gov/tipsadvice/businesscenter/guidance/complying-coppa-frequently-askedquestions.

We hope that your child will enjoy using Seesaw to document and share their learning this year. Please sign below and return this permission slip so that your child can use Seesaw.

————————————————————————————————————

Please sign below and return the form.

I give consent for my child, listed below, to use Seesaw for class activities.
Student Name: _____

Parent Printed Name: _____

Parent Signature: _____Date: _____

Staff loan of school ICT equipment agreement

Staff must comply with the following conditions:

- All school resources (including computers, laptops, tablet devices) and their associated accessories are provided for educational use; they must not be used for any other purposes. Only portable resources (such as laptops and tablet devices) may be removed from school, to facilitate preparation for teaching and learning, in accordance with the details set out below.

Additionally, the resources may not be passed on to any third party.

- All electronic devices are expensive and therefore must be looked after appropriately and must be kept in a safe place, including those taken off site.
- All staff are reminded that the school does not insure property for out of school use. As such it is the responsibility of individual staff taking electronic devices off-site to provide adequate insurance cover for the **full-replacement cost** of the electronic device including software and accessories. This amount can be advised by the Principal or ICT Co-ordinator.
- Users must not give access to any confidential material relating to the school or its pupils without prior consent being granted by the Principal.
- It is the duty of the user to ensure that all passwords and access codes are kept strictly confidential, except where usernames and passwords are kept on record by the ICT Manager.
- All portable devices must be setup on the school's Mobile Device Management (MDM) System by the ICT Manager before being allocated to staff.
- Portable devices should be promptly returned to school at any stage upon request from SLT, ICT Manager or Director of ICT. Staff should be aware that it may be necessary from time to time to wipe the portable devices for performance reasons.
- In the case of Apple devices, staff are advised that use of 'iCloud' should be restricted to a school-registered iCloud ID, setup on each user's Apple device by the ICT Co-ordinator. Staff should not register or enter a personal iCloud ID on the device. These school-registered iCloud ID account details are recorded and securely stored by the ICT Co-ordinator.

Staff wishing to take any electronic device off-site must have signed below to indicate their agreement of these conditions, a copy of which will be retained by the ICT Co-ordinator.

☐ I have read and understood the school's e-Safety, ICT Acceptable Use and Digital Media Policy and agree to abide by this policy.

☐ I accept responsibility for the full replacement value of all equipment which I take off-site.

☐ I have read and understand the conditions contained on this form above and will abide by them.

Please complete and return this form to the Principal.

Staff Name: **(Please Print)**

Signed: **Date:**

Roe Valley I.P.S. Staff, Governor, Visitor and other Adults Working in School Acceptable Use Agreement – ICT Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns of clarification should be discussed with the ICT co-ordinator or the school Principal.

- I appreciate that ICT includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is an offence to use the school ICT system and equipment for any purpose not permitted by its owner.
- I will only use the school's email / intranet / learning platform and any related technologies for uses permitted by the Principal or Board of Governors.
- I will comply with the C2K security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activities carried out under my username
- I will ensure that all school generated electronic communications are appropriate and compatible with my role.
- I will only use the approved, secure school email for any school business
- I will ensure all data is kept secure and is used as appropriately as authorised by the Principal. If in doubt I will seek clarification. This includes taking data off site.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images will only be taken, stored and used for purposes in line with school policy, and with written consent of the parent / carer. Images will not be distributed without consent of the parent/carer, and with permission of the Principal.
- I understand that my permitted use of the internet and other related technologies can be monitored and logged, and can be made available, on request, to the principal.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated or Deputy Designated Teacher for Child-Protection.

I agree to follow this code of conduct, and to support the safe use of ICT throughout the school.

Full Name –

Signature –

Date –

Review

- Review Date - December 2018
- Reviewed annually and updated in consultation with staff, particularly SLT and SENCO
- Presented to and shared with the BOG regularly
- Shared with parents
- In line with whole school learning and teaching policy.