**COMHAIRLE NAN EILEAN SIAR**
**Roinn an Fhoghlaim is Seirbheisean Chloinne**
Department of Education and Children's Services

# POLICY ON E-SAFETY AND ACCEPTABLE USE OF COMMUNICATION TECHNOLOGY IN SCHOOLS

***April 2014***

EDUCATION AND CHILDREN'S SERVICES COMMITTEE:

# Policy on e-safety and acceptable use of Communication Technology in Schools

*What to do if you are worried or concerned about a child or young person?*

*If you are worried or concerned about a child or young person, you should contact the Comhairle nan Eilean Siar Duty Team:* ***01851 701/702*** *or the Police:* ***101***

***Document Control***

| | |
|---|---|
| ***Guardian/Keeper:*** | ***Hamish Budge (Education Support Officer)***<br>***Gordon McKay (Child Protection Officer)*** |
| ***Version Number:*** | ***1.0*** |
| ***Approval Date:*** | |
| ***Publication Date:*** | |
| ***Effective From:*** | |
| ***Review Date:*** | ***Continuous*** |

## INDEX

**EDUCATION AND CHILDREN'S SERVICES DEPARTMENT**

# Policy on e-safety and acceptable use of Communication Technology in Schools

## INTRODUCTION

1.1 This policy document will assist schools in making appropriate choices and to adopt safe practice and responsible use of online technology.

## BACKGROUND

2.1 The Service Statement of Intent includes the following:

- Keep individuals safe and protected
- Develop active and responsible citizens

2.2 The advances in mobile technologies[1] have been rapid in recent years and developments will continue. A mobile device is a long-range, portable electronic device for personal telecommunications.

2.3 The technology enables users to access a wide range of facilities, including phone calls, text, email, photographs, video clips, games, music, internet access, TV programmes and radio. The benefits of such devices are obvious and it is accepted that this is the preferred means of electronic communication. A high percentage of youngsters of all ages and socio-economic groups have their own personal communication devices.

2.4 There are a number of projects and pilot studies presently underway in the UK and across the world where the focus is on using such technologies in a positive way to support learning and teaching in classrooms. This is exciting and is reminiscent of how the world wide web (www) and the internet have developed to support young people's learning.

## CONTEXT

3.1 The Service Statement of Intent includes the following:

"Learning in health and wellbeing ensures that children and young people develop the knowledge and understanding, skills, capabilities and attributes which they need for mental, emotional, social and physical wellbeing now and in the future. Each establishment, working with partners, should take a holistic approach to promoting health and wellbeing, one that takes account of the stage of growth, development and maturity of each individual, and the social and community context.

I can expect my learning environment to support me to:

- learn about where to find help and resources to inform choices
- assess and manage risk and understand the impact of risk-taking behaviour
- reflect on my strengths and skills to help me make informed choices when planning my next steps"

Curriculum for Excellence, Health and Wellbeing

3.2 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

[1] "Mobile technologies" includes mobile phones, Tablet computers, ipods, WiFi-enabled MP3 players and other related devices

3.3 The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times, however they must also be provided with the skills, knowledge and understanding to protect themselves from any online risks. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying [2]
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

3.4 It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings

3.5 This Policy document aims to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with school behaviour, anti-bullying and child protection policies.

## MOBILE TECHNOLOGIES – GUIDANCE FOR SCHOOLS

### School Context

4.1 Increasing numbers of young people carry communications devices to school in the same way that they carry pens and pencils. However, even the basic use of a phone in a school environment intrudes on other people and should be used with due care and within the appropriate rules.

### School Policy

4.2 Communications devices should only be used in schools according to this policy framework. Alerting pupils to their rights and responsibilities should be managed as part of citizenship, health and well-being and personal and social education.

4.3 It is recommended that the normal consultation process regarding policy formulation is continued and staff, pupils and parents are engaged in the process as appropriate. Parental engagement and co-operation is likely to support successful implementation of agreed policy as well as apprising them of the outcomes should the policy be abused. It is understood that, whilst the key principles are the same for all schools, the operational aspects of the policy may differ slightly depending on the age of the pupil and/or the size and location of the school.

4.4 The majority of young people use communications devices appropriately and abide by existing rules. However an increasing number of pupils are misusing such devices and are possibly unaware that they may also be breaking the law. Clearly stated policy is necessary to ensure the safety and protection of all people on school premises, staff as well as pupils. It is the responsibility of all members of staff to implement the agreed policy.

[2] "cyber-bullying" includes the use of mobile phones and other related devices, and also e-mail to abuse, threaten or otherwise distress another person

**Pupil Rights**

4.5 Parents provide their children with a communications device for a variety of reasons including personal safety. It is the right of a pupil to bring a personal mobile phone to school with the clear understanding that the individual pupil is responsible for its care and usage.

4.6 In the case of younger pupils, the parent/carer should be clear that the phone is ultimately the responsibility of the child and not the teacher or another staff member. Primary schools however may choose to gather in mobile phones during the school day. Such operational aspects are at the discretion of the individual school.

4.7 Communications devices should be switched off in classrooms and whilst moving between classes except as part of a planned programme of learning or in agreed exceptional circumstances. Individual establishments may be more specific depending on the age of the pupil, the timing of the school day and physical environment.

4.8 Pupils may use communications devices at intervals and at lunchtimes, unless a pupil is banned by the school.

**Pupil Responsibilities**

4.9 It is the pupil's responsibility to ensure their device is switched off in accordance with school policy.

4.10 Bullying and harassment of pupils and staff are unacceptable in any form in school and this includes the use of communication devices.

4.11 The use of communication devices during breaks and lunchtimes is acceptable on the understanding that the school behaviour policy as well as the communications policy is respected.

4.12 Inappropriate use of communication devices to take photographs, audio and/or video clips of other pupils/staff without individual permissions is not permitted in a school context.

4.13 Pupils should not download unsuitable material.

4.14 It is an offence to forward images/materials of a pornographic nature. Young people should be made aware of such aspects of the law.

**Policy Breaches**

4.15 Schools should clearly state the possible consequences of violation of the policy.

4.16 Members of staff may confiscate devices which are used in breach of school policy and procedures. Should devices require to be confiscated then school procedures and protocols should be explicit and known to all pupils, staff and parents. Members of staff who confiscate a device must follow these procedures, particularly with respect to the treatment of potentially private, indecent images and secure storage. Staff duties with respect to confiscation should be clearly stated in the school handbook.

4.17 Devices must always be returned to the pupil if appropriate, parent, or in exceptional circumstances, the police.

4.18 Persistent violations of school policy may result in a pupil losing the right to carry a communications device on school premises. Discussion with parents/carers would be crucial prior to this happening. Such repeated violations of school policy (or very serious individual breaches) may also result in serious disciplinary sanctions (including exclusion from school) being applied. The police may also be required in certain serious cases.

### School Data Security Policy

4.19 Ensure data is kept safe and secure by complying with the School Data Security Policy.

### Health and Safety

4.20 Research into the safety of communications devices has produced inconclusive results although most experts agree that it is sensible to limit the use of mobiles by young children. Therefore, it is a parent's decision to provide a child with a communications device.

### Social Networking Sites

4.21 Many devices give access to internet-based social networking sites. Whilst an integral part of the social, leisure and increasingly the academic existence of almost all young people. They present some significant challenges in terms of cyber-bullying. If such sites are to be used, appropriate guidance, vigilance and prompt action are essential.

4.22 There are also inherent risks in the use of such sites for teachers with respect to the potential overlap between their personal and professional lives. See Section 6: Moderation Guidelines for Social Media

### Child Exploitation and On-Line Protection (CEOP)

4.23 CEOP is a Government agency whose work is centred on protecting children and young people from exploitation using on-line media or websites.

4.24 Training in protecting children and young people from on-line exploitation is a part of the service provided to staff and pupils and offered to parents by the Comhairle.

4.25 Through this training, all staff will become more aware of the significant potential dangers posed by a range of on-line social and leisure sites. Since many devices now support access to such sites, it is important that school policy addresses these issues. Again, it must be noted that vigilance and prompt action are essential.

## SCHOOL ADVICE TO MEMBERS OF STAFF ON THE USE OF SOCIAL NETWORKING SITES

### School Guidelines for Mobile Communications Technology

5.1 In order to protect the safety of our staff in school, the following guidelines are offered for the use of mobile communications technology and social networking sites.

### Social Networking sites

5.2 As a council employee it is important to be aware that posting information or views about the council in a personal capacity cannot be isolated from your working life. Any information published online can, if unprotected, be accessed around the world within seconds and will be available for all to see. This activity contributes to your online digital footprint – a traceable and searchable history of your on-line activity. It can potentially been seen by anyone, anywhere in the world.

- Remember you are personally responsible for any content you publish. Employees must not disclose any confidential information relating to the business of the Council, for example, if it would compromise a right of personal or commercial confidentiality. Such action would be in breach of the Employee Code of Conduct and may lead to disciplinary action.
- When using social media for personal purposes you must not state or imply that you are speaking on behalf of the Council. If an employee wishes to set up his/her own personal blog, website or web presence, they must use a disclaimer that protects the Council e.g. 'these are my personal views and not those of my employer'

- Employees must consider carefully whether it would be appropriate to befriend someone when using social media for personal purposes, for example where there is a professional/client/pupil relationship, and/or where this could create a potential conflict of interest.
- Do not use your Council email address to sign up to social media sites for personal use
- any communications with pupils should not stray into what could be considered inappropriate on your behalf; If a pupil discloses something that could be a child protection issue, you have a duty to report this in school.

**Mobile Phones including Smart Phones (and similar devices)**

5.4 It is not recommended that you give your mobile number out to any parent or pupil. If there is a situation where pupils will need a mobile number to contact you on (e.g. for a school trip), we recommend that the department purchases a pay-as-you-go phone for use on such occasions.

5.5 It is also not recommended that you have pupils' mobile phone numbers on your personal phone because of potential loss or theft.

5.6 It is recommended that you keep your Bluetooth facility switched off in school, in case you inadvertently receive something intended for someone else. Do not bring your phone into school if there are any files on it that would cause you embarrassment if they got into the wrong hands.

5.7 In keeping with school policy, pupils should not have their mobile phones on in your class. If you see someone who does, ask them to switch it off. Extreme caution should be taken before you confiscate a phone and in handling the safety/security of the phone after confiscation. If it goes missing whilst in your possession, you will be responsible. Also, do not leave a confiscated phone on someone else's desk with a note (in the hope that they will return and lock it away for you) – you are still responsible if it goes missing. Until you have seen it safely transferred to a place of safe-keeping, you are the responsible member of staff.

5.8 Do not allow pupils to take photos of you or others in your class, or to make videos using their phones, or other devices (Unless part of a lesson). If you catch someone doing this, ask them to delete it and check they have done so. If they refuse, or you are in any doubt, refer this to your PT, who may decide to refer on to the Headteacher. If you see that a pupil has inappropriate material on their phone, take possession of the device and urgently seek advice from your PT, the pupil's guidance teacher or designated child protection officer. **Never** print or send the image to someone as this is also an offence.

**Email**

5.9 For similar reasons to the Social Networking advice, it is not recommended that you give pupils your personal email address. If you need pupils to email you homework, etc, you can give them your GLOW address.

**Websites/wikis/blogs/on-line gaming/dating sites/etc.**

5.10 While you are at liberty to post what you like on the internet as an individual in your own time, again it is recommended that you ensure that anything that you post should not cause yourself, the school or the authority awkwardness or embarrassment if a pupil were to access it.

5.11 You should be aware that both the GTC and The Comhairle Codes of Conduct apply here. You should also be aware that certain aspects of the misuse of devices may require the implementation of Child Protection procedures and a referral to the Child Protection coordinator.

5.12 If you see (or are made aware of) anything inappropriate about yourself, another member of staff, a pupil or the school in general on a website, please refer this immediately to the designated Child Protection Officer for investigation.

Your designated Child Protection Officer is: _____

**MODERATION GUIDELINES FOR SOCIAL MEDIA**

**Breaking these guidelines could result in the following:-**

6.1 Removal of Internet or computer access for a period or permanently, and may also involve referral to parents/carers, local authority and/or police.

**Defamation is not allowed**

6.2 Defamation is the legal term that covers both slander and libel; slander is defamation by word of mouth, and libel is defamation in written form. A defamatory comment is one that may damage or undermine the reputation of another.

**Harassment: Privacy Law**

6.3 Individuals or groups must not blatantly harass other individuals or groups.

**Racism**

6.4 Anything that may be seen to be racist and offensive towards any group of people is not allowed.

**People with Disabilities**

6.5 Reference to disability should be included only in neutral terms. Stereotyping messages will not be accepted.

**Minority Groups**

6.6 Do not post messages that may offend minority groups. Only positive, factual, non-confrontational and constructive comments are allowed.

**LGBT**

6.7 It is acceptable for a user to refer to his/her sexuality or gender identity. It is not acceptable for users to use terms associated with sexuality or gender identity in a negative way.

**Obscenity and Indecency**

6.8 Any obscene material, relating to race, religion and offensive sexual material will be removed (this includes threats, harassment, incitement, abuse, swearing, religious hate, etc…).

**Personal Detail Exchange**

**6.9** **Do not** post public messages submitting or asking for any contact details of any sort; be it mobile, home or any other contact telephone numbers, e-mail addresses, surnames, school names or locations or arranging meeting times and place.

**No Geographic / Location References**

6.10 It is fine for users to mention their town, city or education establishment but any further location details should not be used.

**Users Arranging to Meet Up**

6.11 **Do not** enter any discussion which involves users trying to meet or discussing any form of location details.

**Contempt of Court or other Criminal or Immoral Activity**

6.12 Do not post comments on court proceedings and avoid any discussions concerning criminal or immoral activity.

**Drugs, Smoking and Alcoholic Drinking**

6.13 Do not post messages which advocate or encourage the use of, or selling drugs, smoking or alcohol.

## UNACCEPTABLE USE OF COMMUNICATION TECHNOLOGY

7.1 The school and Council networks and/or stand-alone computers or other ICT devices may not be used by pupils, staff or other users within the school for any of the activities described below:

- Your use of the school's computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use school computing services to inconvenience, annoy, harass, libel, defame, slander, intimidate, impersonate or otherwise abuse another person.
- You must not create or transmit defamatory material.
- You must not use school computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for academic purposes which would require the fullest disclosure and special authorisations)
- You must not use the school's computing services to conduct any form of commercial activity without express permission.
- You must not use the school's computing services to disseminate mass (unsolicited) mailings.
- You must not create or transmit material with the intent to defraud others.
- You must not use the ICT facilities for personal financial gain, gambling, political purposes or advertising.
- You must not create or transmit material which infringes the copyright of another person or organisation.
- You must not install, use or distribute software for which you do not have a license.
- You must not create or transmit unsolicited bulk or marketing material to other users of networked facilities or services.
- You must not use your mobile phone smart phone or similar device (e.g. iPad, Netbook etc.) for communications, photography or other purposes during lessons, other than as an agreed part of the teaching and learning process.

**Using External Web 2.0 Services**

7.2 The following points should be noted when using external web 2.0 services

**Pros**

- They offer ready access to the latest, flexible technology.
- They offer opportunities to explore responsible use
- They provide a platform to explore and improve digital literacy
- The social aspects of many services are enhanced by very widespread usage
- They offer routes to worthwhile teaching and learning experiences such as research collaboration or peer-to-peer group interaction.

**Cons**

- It is easy to be tempted to produce, and submit, content to such sites that you might later regret.
- What content or comments you do submit becomes potentially available across the world.
- It is difficult, but important, for teachers (and pupils) to maintain complete separation between their private and work usage.
- Such content may have a longer life span than you might have imagined and could be accessed by a wide audience, including potential employers.
- Although such sites are external to the school, the way in which you use them, or the content that you submit to them might still lead you into trouble with the school/authority and their policies and regulations.

Acknowledgements The beXcellent project Olympic.org

7.3 Members of staff should always read and consider the terms and conditions for any service they register with and ensure that they understand the implications of the service conditions. You are still bound by the general conditions above if using such services. Staff should check with the responsible member of the senior management team before proceeding with subscription to such a service.

7.4 Pupils may only use such services as identified by the Principal Teacher of the subject concerned, with the permission of the designated member of the senior management team.

7.5 The school reserves the right to block access to such services, whether for pupils or staff, should there be a potential or actual compromise of terms of the general conditions above.

**Monitoring and Logging**

7.6 Activities regarding network transactions will be monitored, randomly inspected, logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available only to authorised systems personnel and kept for no longer than necessary and in line with current data protection guidelines.

7.7 Such records and information are sometimes required - under law - by external agencies and authorities. This school will comply with such requests when formally submitted.

# Appendix 1: Responsible Use

*(Can be adapted in consultation with stakeholder)*

**Parent's Letter**

**Responsible Internet Use**

As part of your child's curriculum and the development of ICT skills your school is providing supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavor is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, we feel that the pupils themselves must also play their part. For this reason we have drawn up a list of Net Rules for Responsible Internet Use which we ask pupils to agree to, and abide by.

The reasons for their introduction have also been explained. It has been pointed out to the children that anyone deliberately breaking the rules will have their personal access to the internet within school either denied, or at least severely restricted.

I have attached a copy of these rules for your information and you may wish to discuss them again with your child.

Once you have read this letter and the attached rules, we ask that you and your child sign the permission/agreement form below and return it to the school.

If there are any aspects of internet use you wish to discuss (either before you sign the form, or at any time in the future) please feel free to contact the school.

Yours sincerely

Headteacher

**Parent / Guardian's permission**

I give permission for access to the internet set out in the above letter.

**Signed:**

**Date:**

**Print name:**

**Pupil's agreement**

I agree to follow the Net Rules.

**Signed:**

**Date:**

**Print name:**

# Appendix 2: Net Rules

*(Can be adapted in consultation with stakeholder)*

## These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my own network login and password, which is secret.
- I will not delete or look at others people's files without permission.
- I will only email people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an email or an email attachment sent by someone I do not know.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

## Remember it is not your fault if you get a message like this.

- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

# Appendix 3: Safe Use of Technologies Within School

*(Can be adapted in consultation with stakeholder)*

| | STAFF / OTHER ADULTS | | | | STUDENTS / PUPILS | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | ✓ | | | | ✓ | | | |
| Use of mobile phones in lessons | | | | | | | ✓ | |
| Use of mobile phones in social time | ✓ | | | | | ✓ | | |
| Taking photos on mobile phones or other camera devices | | ✓ | | | | | ✓ | |
| Use of handheld devices eg: ipod, PSPs | ✓ | | | | | | ✓ | |
| Use of personal email addresses in school or on school network | ✓ | | | | | | ✓ | |
| Use of school email for personal emails | | ✓ | | | | | ✓ | |
| Use of instant messaging | | ✓ | | | | ✓ | | |
| Use of social networking sites | | ✓ | | | | | ✓ | |
| Use of blogs | ✓ | | | | | | ✓ | |

# Appendix 4: Whole School Approach to the Safe Use of ICT

**Whole School Approach**

1.0 Within school, creating a safe ICT learning environment includes three main elements:

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

*Reference: E-safety Developing whole-school policies to support effective practice*

**Roles and Responsibilities**

2.0 e-Safety is recognised as an essential aspect of strategic leadership within the school and we aim to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

**Our school e-Safety Co-ordinator is ……..**

2.1 The e-Safety Coordinator ensures that they keep up to date with e-Safety issues and guidance through liaison with local authority staff and through contact with organisations such as The Child Exploitation and Online Protection (CEOP) . The school's e-Safety coordinator ensures the Headteacher, senior management team, staff and parents are updated as necessary.

2.2 All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

2.3 All staff should be familiar with school policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- Their role in providing e-Safety education for pupils;

2.4 Staff are reminded / updated about e-Safety matters at least once a year.

**How will complaints regarding e-Safety be handled?**

3.1 The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

3.2 Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by Guidance staff / Senior management / e-Safety Coordinator, Headteacher
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to local authority / police.

3.3 Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse must be referred to the Headteacher.

3.4 Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school and Western Isles Inter-Agency Child Protection Procedures.