Magherafelt Learning Partnership

Electronic Communications

Safe Guarding Guidance for School Staff

2016-2018

Contents

1. Introduction.

First and foremost this guidance is provided to protect school staff from harassment, real or alleged misuse and any consequential disciplinary action arising from the use of electronic communication equipment in or outside school. It is also intended to ensure that the school's equipment is used responsibly and safely at all times. There are implications for the actions of individuals and the school as a whole.

This document is part of the school's E-Safety policy and Acceptable Use agreements.

Electronic communications equipment includes (but may not be limited to) telephone, fax, voicemail, computer, laptops, internet, mobile phone (all types), photocopier, digital cameras, web cameras, videos and palm-held equipment. Types of communication can include (but may not be limited to), phone calls, e-mail, text messaging, multimedia messaging, transmission of photographs and moving pictures, contact via websites and social network sites, blogging, wikis, contact via web cameras and internet phones.

Staff will sign the Acceptable Use Policy to show they have understood and accept the contents of this document

Failure to follow any aspect of this guidance (either deliberately or accidentally) could lead to disciplinary action in accordance with the school's disciplinary policy which ultimately will result in dismissal.

2. Safe and Responsible Use.

2.1 The Internet.

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through:

- access to world-wide educational resources, including museums and art galleries.
- access to experts in many fields for pupils and staff.
- educational and cultural exchanges between pupils world-wide.
- collaboration between pupils, professionals and across sectors.
- access to learning wherever and whenever convenient.

The Internet enhances the school's management information and business administration systems through:

- communication systems.
- improved access to technical support, including remote management of networks and automatic system updates.
- online and real-time 'remote' training support.
- secure data exchange between local and government bodies.

In support of this, the government funds C2k to provide this infrastructure, supporting software, maintenance and training.

The Risks.

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is totally unsuitable for pupils.

In line with school policies which protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse. Risks can be high outside school, so this school provides an education programme for parents/guardians.

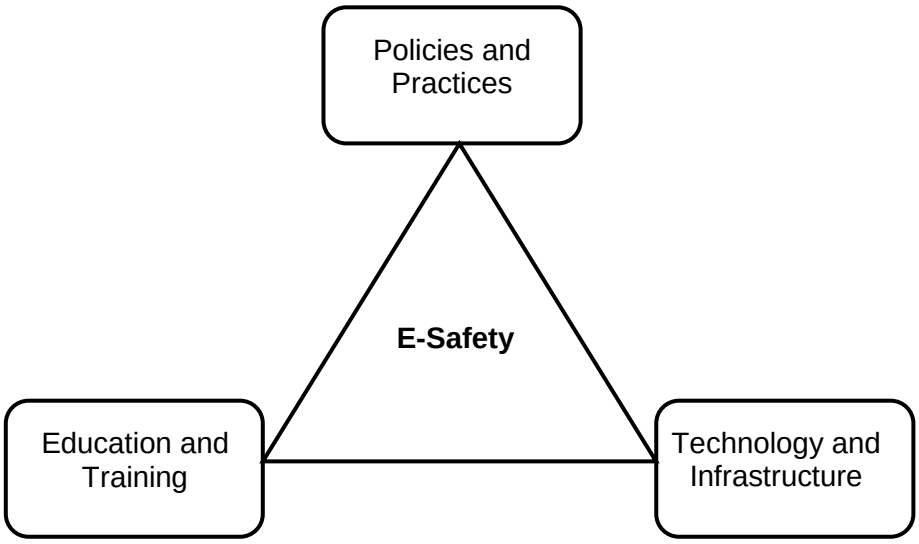
Schools also need to protect themselves from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child

pornography on computers or to use Internet communication to 'groom' children. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Users within this school are informed that the use of school equipment to view or transmit inappropriate material is "unauthorised" and those who infringe will be subject to the school's disciplinary procedures. Furthermore the school will take all reasonable and appropriate steps to protect pupils, staff, parents/guardians. Reasonable steps include technical and policy actions and an education programme for pupils and staff and parents/guardians.

In formulating its E-Safety Policy the school has considered the three core elements of:

- Technology and Infrastructure.
- Policy and Practices.
- Education and Training.



Schools in Northern Ireland have access to a secure and managed network provided by C2k. This service provides: approved firewall solutions, up-to-date anti-virus, anti-spyware and anti-spam software; Individual log-ins, coupled with Auditing software, meaning network activity can be monitored and logged, providing a secure network.

2.2 E-mail.

Schools in Northern Ireland have appropriate educational, filtered internet-based e-mail options through the C2k system.

In the school context e-mail should not be considered private and the school reserves the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

An individual should not access the e-mail of another individual within the school without express permission and a clear understanding of the reason for the proxy access.

All work-related e-mails should be written using a school e-mail address. School e-mail should be regarded as an official communication tool. E-mails should be written in the same professional tone and text as any other form of official school communication

If e-mail is used as an official means of communication with parents, government organisations, educational institutions etc then copies should be kept as a record of the communication. This could be achieved by saving or printing a copy, forwarding the e-mail to the school office or other relevant staff.

E-mail attachments should be opened with care unless the receiver has absolute confidence in its origin as this is one of the most likely points of introducing a virus into a computer system.

The sending of racially abusive or other offensive email is forbidden and may be considered a criminal act. It should be borne in mind that emails may be submitted as evidence in legal proceedings and that e-mail discussions with third parties can constitute a legally binding contract.

E-mail must not be used by staff to transfer information about pupils – unless it is within an encrypted, secured e-mail system.

It should be remembered that the data (in e-mails or other systems) does not belong to the User but to the organisation. The User can only use the data with the permission of the Principal (or other approved person) and only for the purposes for which they received permission. Therefore a school user could be personally liable for breaching the Data Protection Act (DPA98) if personal information was disclosed because of their unauthorised actions.

Personal e-mail addresses of users within the school not published on the school website. Group e-mail addresses are used for communication with the wider public.

(a) Pupils

The school will ensure that pupils:

- are made aware of the risks and issues associated with communicating through e-mail and the strategies in place to deal with inappropriate e-mails.
- understand good 'netiquette' style of writing and appropriate e-mail behaviour.
- are introduced to e-mail and can only use the school domain e-mail accounts on the school system.
- are taught about the safety and 'netiquette' of using e-mail both in school and more generally personal accounts at home:
    - not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/guardian.
    - that an e-mail is a form of publishing where the message should be clear, short and concise.
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
    - they must not reveal private details of themselves or others in e-mail, such as: address, telephone number, etc.
    - to 'Stop and Think Before They Click' and not open any attachments unless they are sure that the source is safe.
    - the sending of multiple or large attachments should be limited.
    - personal information should not be sent as attachments on open e-mail. A secure method of encrypted transfer should always be used.
    - embedding adverts is not allowed.
    - that they must immediately tell a teacher/responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
    - not to respond to malicious or threatening messages.
    - not to delete malicious of threatening e-mails, but to keep them as evidence.
    - not to arrange to meet anyone they met through e-mail without having first discussed with an adult and taking a responsible adult with them.
    - forwarding of 'chain' e-mail letters is not permitted.

Pupils sign the school Pupil AUP to say they have read and understood the e-safety rules, including e-mail and that any breach of the agreement will have consequences.

(b) Staff.

The school will ensure that staff know that:

- there are risks and issues associated with communicating through e-mail and are familiar with the strategies in place to deal with inappropriate e-mails.
- they are allowed to only use the school domain e-mail accounts on the school system.

- they can never use email to transfer staff or pupil personal data. Data transfer is by secure system only.
- they cannot access personal e-mail during the school day.
- e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.
- the sending of multiple or large attachments should be limited.
- personal information must not be sent as attachments on open e-mail. A secure method of encrypted transfer should always be used.
- the sending of chain letters is not permitted.
- embedding adverts are not allowed.

All staff sign our school Staff AUP to say they have read and understood the e-safety rules, including e-mail and that any breach of the agreement will have consequences.

(c) Inappropriate E-mails.

- It is impossible to control what information is sent to a member of staff by e-mail. However if offensive, obscene and/or discriminatory material is received it is then the responsibility of the receiver to report immediately, and in writing, to the designated person in school (or the head teacher). Never send a reply.
- Keep a printed copy of the e-mail as evidence and pass a copy of the e-mail to the appropriate person (Complaints Officer) for the record. Ensure that the sender's information is also recorded as their e-mail service provided may take action.
- E-mails which are particularly disturbing or break the law will be reported to the Police.
- Messages relating to or in support of illegal activities will be reported to the relevant Authority and Police.

2.3 Social Networks, Blogs and Wikis.

(a) Social Networks.

Social networks such as 'Instagram, 'Facebook', 'Twitter', are popular with staff and students. However:

- neither staff nor pupils should use school facilities to access or update their personal social networks.
- no personal information should ever be added to a user's social site.
- staff and pupils should be careful as to who they add as 'friends'.
- comments made on a social network site which relate to the school or pupils in the school have the potential to be misinterpreted and could result in disciplinary action.
- photographs and descriptions of activities in the personal life of staff in particular and other members of the school community in general may not be considered appropriate if viewed by other staff, pupils or parents.

- users should be aware that even if they have used the privacy settings, they may not be able to prevent material becoming public from their 'friends' sites.

(b) Blogs, Wikis.

It is recognised that these online communications tools, such as weblogs ("blogs") and Wikis, have a potentially useful role in schools – such as on school websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where pupils and their families are sharing these tools with staff in school it is important that this should always be through a school based provision, such as the school VLE using a school log-in where all communication is open and transparent.

If staff keep personal blogs the content must maintain acceptable, professional standards. Any inappropriate use may lead to disciplinary action in accordance with school policy. All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school or the Magherafelt Learning Partnership.

Schools are also vulnerable to material being posted about them online and all users should be aware of the need to report this should they become aware of anything bringing the school into disrepute. Schools should regularly check to see if any such material has been posted.

(c) Threatening or Malicious Material Published Online Concerning a member of the school or the school itself:

- Secure and preserve any evidence. For example note the web address (URL) or take a screen shot or copy and print the screen.
- Report immediately to the e-Safety Officer or Head Teacher.
- Contact the up-loader of the material or the Internet Service Provider/Site Administrator and ask for the material to be removed.
- If the material has been created by a member of the school community or a parent then the school will investigate and implement the school's disciplinary policy if appropriate.

All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others.

2.4 Real Time Online Communication - Web Cameras, Chat, Mobile Phone.

The ability to communicate in real time using the computer and other electronic devices (such as mobile phones) makes these an excellent tool for a range of educational purposes. However, staff should take the same level of care with these tools as they would if working in a face to face situation with a student or group of students. Access should always be through a school created account, never a personal account and it should be focused on a clearly specified educational objective.

There are likely to be times when this kind of activity will be organised by a member of staff to be outside normal school hours and off the school premises. In this situation it

should always be carried out with the full knowledge and agreement of the member of staff's line manager. Staff should be aware that they must remain focused on the educational purpose of the communication and never allow it to become a social occasion.

Staff should also agree to specific times for availability and only allow contact during these times, to protect their personal time. When a web camera is used it should have a clear purpose. Staff should be aware of the ability of meetings of this kind to be recorded without their knowledge.

Staff must protect their privacy by never allowing pupils or parents to obtain their mobile phone number or leave their mobile phone where it could be accessed by a pupil. Cyber-bullying of both staff and pupils is very common by mobile phone.

Action initiated in the event of an e-safety incident.

- If a pupil is the victim report immediately to a teacher or other responsible adult. If a teacher report immediately and in writing to the teacher's line manager.
- Don't reply to abusive or worrying text or video messages.
- Don't delete messages. Keep them for evidence.
- Use 1471 to try and obtain the number if possible. Most calls can be traced.
- Report it to your phone provider and/or request a change of number (see Appendix E in main document for list of phone numbers).
- Technical staff may also be able to help by finding or preserving evidence such as logs of the call.

3. Misuse of electronic equipment.

Misuse is a serious disciplinary offence. The following examples of misuse apply to all members of the school community.

(a) Staff and pupils MUST NOT use school equipment (including a school provided laptop) to:

- Store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred.
- Gamble.
- Download or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright.
- Spend school time on personal matters (for example, arranging a holiday, shopping, looking at personal interest websites).
- Store personal information on the school network that uses up capacity and slows down the system (for example, personal photos, screensavers or wallpaper).
- Send e-mails, texts or messages or publish anything on a website, social networking site or blog, which:
  - is critical about members of the school community including pupils.

  - contain specific or implied comments you would not say in person.
  - contain inappropriate comments which could cause offence or harassment on the grounds of gender, race, disability, age, religion or sexual orientation.
  - have originated from a chain letter.
- Conduct private and intimate relationships via e-mail.
- Download or copy software (excluding software updates) or use the e-mail system to transmit any documents or software without checking copyright or licence agreement.
- Install software licensed to the school on a personal computer unless permission to do so is explicitly covered by the school licence agreement.
- Take, transmit or publish pictures of a member of staff or pupil on your mobile phone, camcorder or camera without the person's permission.
- Give away e-mail lists for non-school business. If in doubt, ask the Head Teacher.
- Use internet chat rooms (other than the secure, moderated facilities which are provided within the school's VLE).
- Do anything which brings the school into disrepute.

(b) Personal Laptop.

A personal laptop:

- brought onto the school premises MUST NOT be used to undertake any of the activities in (a) above during the school day.
- should not have information stored within it which would be deemed to be unacceptable on a school machine.
- used at school should have a separate secure account for use whilst at school.
- used for any school activity must be fully protected against virus infection.

4. Monitoring and Privacy.

The school's e-mail and internet facilities are systems, provided by the Department of Education to the school and managed by C2k. The school therefore reserves the right to monitor all use of the internet and of the school's ICT systems. Usage will be monitored to ensure that the systems are being employed primarily for educational reasons, that there is no harassment or defamation taking place and that all members of the school community are not entering into any illegal activities. Electronic equipment on the school site may be searched and examined.

All users need to be aware that internet sites visited are traceable and that deleted messages or attachments can be recovered.

E-mail, telephone calls and internal and external post (unless clearly identified as private and confidential post) should be used primarily for educational reasons. To ensure this monitoring will be carried out as deemed appropriate.

Any material stored on the school's network or being circulated via the school's e-mail system has no rights of individual privacy. In accordance with RIPA (Regulation of Investigatory Powers Act 2000) monitoring or surveillance without a user's knowledge can be carried out on internal e-mail systems, or information stored on a server. It is

permitted to intercept communications in this way so the school can ensure its systems are being used properly in accordance with school policies and are working correctly.

5. Breaches and Sanctions.

Failure to follow any aspect of the school's E-Safety policies (either deliberately or accidentally) could lead to disciplinary action in accordance with the school's disciplinary policy which may ultimately result in dismissal.

6. Good practice guidance for school staff.

- Pay close attention to the list of misuses in **Section 3** because this list is for your protection and clarifies how possible disciplinary action can be avoided.
- In communications with pupils and parents, never give out personal information which identifies your home address, phone number, mobile phone number or personal e-mail address. Once such information is known you are open to harassment through unwanted phone calls, text messages and e-mails.
- Protect your social network site by using the correct privacy settings. Make sure that personal information cannot be seen from the links to your friends' sites.
- Do not accept pupils as friends on your personal social network site. If at all possible do not include parents as friends.
- Avoid the use of chat rooms, instant messaging or other social networking services which are accessed socially by pupils and are not monitored by the school.
- Always keep a copy of e-mail communications with pupils and parents (whether sent or received) and keep a note of the dates, times and content of telephone conversations.
- If your school laptop is used outside school for non-school activities then set up a different user account to ensure that personal or confidential data is protected. Use a strong password to protect the school laptop from unauthorised access.
- Make sure you do not allow people to see personal or confidential school information when a computer is left unattended. Turn it off, log off and set up a password-protected screen saver to prevent unauthorised access.
- Keep all passwords and login details strictly private and always remember to log off correctly after using the computer. Never allow anyone else to use your personal login detail as you will then be held responsible for their online activity.
- Always use the school's digital camera or video camera for taking pictures and upload them onto a school computer. Once uploaded, the images should be deleted from the camera's memory. Photographs of children should not be taken home to use on a personal computer.
- The use of hand held 'walkie- talkies' is increasing in schools. Staff using this equipment should speak professionally and respect confidentiality. Be aware that the message could be overheard.
- If you are using school electronic equipment off site then take the same level of care as you would in school. A digital camera taken off site should not be returned to school with personal photographs on it.

- It is not recommended that personal financial transactions are made on school equipment as information may become accessible to pupils.
- Observe sensible precautions when taking photographs which may include pupils. Always obtain students and/or parental permission and make sure that individual pupils cannot be identified by name, especially, if the photograph is for use on the school web site or VLE. (Refer to school policy for further guidance on this issue.)
- Report immediately, and in writing, to the designated person in school (or your Head Teacher) any web pages accessed or emails received where the content could be described as inappropriate or malicious. Keep copies as evidence.

7. School responsibilities.

In order to ensure safe practice for staff and pupils the school should:

- make it clear that the school will enforce policies to protect staff and pupils from malicious use of mobile phones, in particular the use of camera and video- phones.
- ensure that the school's policy and procedures for home-school communication are shared with all staff.
- establish whole school systems for storing emails, dealing with inappropriate messages and breaches of security.
- provide all staff with a personal e-mail address to be used for all school-related communications.
- establish a clear school policy for monitoring use of the school's electronic equipment by staff and pupils, including procedures for accessing e-mail and files when staff are absent due to holiday, illness, etc.
- provide digital cameras and mobile phones which can be borrowed by staff as required for all school-related work.
- provide a safe learning environment, such as, a VLE for electronic communications with pupils.
- ensure that systems are established for reporting unwanted or accidental electronic communications and that staff and pupils know the correct person to report to should any issues arise. Accurate records must be kept and all incidents treated seriously.
- create procedures to regularly check the school's presence on the web to ensure material detrimental to the school is not published.