KILRONAN
SCHOOL

Policy for E-safety and Acceptable Use of the Internet and Digital Technologies

Updated January 2016

This policy is informed by DE guidance
(DE Circular 2007/01 Use of Internet and Digital Technologies in Schools)

Rationale

At Kilronan School, we understand the responsibility to educate our staff and school community on E-safety issues, to enable them to remain both safe and legal when using the internet and related technologies. Being e-safe while using these technologies relies on selecting appropriate privacy levels, knowing how to behave online and understanding the risks of using the internet and mobile technology: having the tools and knowledge to be able to work safely.

Aims

- To ensure a consistent approach to e-safety issues by all members of the school staff including teachers, classroom assistants, and all ancillary staff.
- To define the roles and responsibilities and legal duties within the school concerning E-safety
- To implement and deliver e-safety education and training in the school for pupils and staff
- To consider the wider issues of e safety within the school community

Use of data outside of school premises

Everybody in the school has a shared responsibility to ensure that any data removed from school is kept securely. All information should be stored in My Files through www.c2kschools.net or if this is not possible, on an encrypted USB or external hard drive and laptops should be password protected by the user. Staff must use these methods of storage for such data, otherwise no other sensitive information should be removed from school.

ROLES AND RESPONSIBILITIES

Board of Governors.
Their responsibility will be to:

- Support the development and on-going review of the e-safety policy and training programme.
- Ensure they are fully aware and adequately trained to deal with any e-safety related incident
- Liaise with the Designated Teacher and Deputy Designated Teacher for Child Protection.

The Principal
Her responsibility will be to :

- Monitor the use of the C2K network by all staff and pupils
- Contact the parents of any pupils involved in the misuse of the network.
- Carry out appropriate disciplinary procedures.
- Inform the Board of Governors about any incidents or concerns.
- Agree with BOG any appropriate pastoral or disciplinary measures to be taken
-

Monitoring
All internet activity is logged by the school's internet provider (C2K). Logs may also be monitored by the ICT co-ordinators and the school principal. All staff and governors are required to read and sign the Acceptable Use Agreement/E-Safety Rules (Appendix 1)

Breaches
A breach or suspected breach of policy by a school employee or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach by staff is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, by the Education Authority. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting
Any security breaches or attempts and any unauthorised use or suspected misuse of ICT must be reported immediately to the Principal or Vice Principal. Additionally, all lost or stolen equipment or data, virus notifications, unsolicited e-mails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to: Mrs Millar (Principal) or Miss Brown (Vice Principal).

E-mail
The use of e-mail within school is an essential means of communication for staff.

- All staff have their own C2k e-mail account to use as a work-based tool. By using your own school e-mail account you are clearly identified as the originator of a message.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients all mail is filtered and logged.
- Staff should not contact pupils, parents or conduct any school business using personal (non c2k) e-mail addresses.
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- All emails which include personal information about a pupil or member of staff must be encrypted.
- Staff must inform the Principal and Vice Principal (Mrs Millar and Miss Brown) if they receive an offensive e-mail.

E-safety
This policy is linked to the Safeguarding and Child Protection policy and the school's code of conduct. ICT and on-line resources are increasingly used across the curriculum. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- All staff will have been given a paper copy 'Kilronan School E-Safety Protocols' (Appendix 2) produced by the Designated Teacher and Deputy Designated Teachers' for Safeguarding and Child Protection.
- Staff receive information relating to e-safety through the ICT and Child Protection team.
- E-safety posters are prominently displayed throughout the school.
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Principal/VP/ICT co-ordinator.
- Deliberate access to inappropriate materials by staff will lead to the incident, depending on the seriousness of the offence:
  - being investigated by the Principal/C2K/Education Authority
  - possible immediate suspension
  - possibly leading to dismissal and involvement of police for very serious offences.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are asked to read through the e-safety trifold leaflet (Appendix 3).
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken for use in school/website/FaceBook page/media.
- Through the Registration/Re-Registration form, parents/carers are expected to sign a Home School agreement containing the following statement:
  'We will support the school e-safety policy to on-line safety and not deliberately upload or add any images, sounds or text that we do not have permission to share or could upset or offend any member of the school community'.
- The school disseminates information to parents relating to e-safety where appropriate in the form of Information evenings, newsletters, the school website and Facebook page.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff should use their own personal passwords to access computer-based services. Staff should only disclose your personal password to authorised ICT support staff (Ms B McCloy or Mrs Ambrose) when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

Safe Use of Images (taking, publication and storage of images)

Digital images are easy to capture, reproduce and publish and therefore, issue. We must remember that it is not always appropriate to take or store images of any member of the school community or public without first seeking consent and considering the appropriateness.

- The school permits the appropriate taking of images by staff with school equipment only with the written consent of parents/carers and staff.
- Staff are not permitted to use personal digital equipment such as mobile phones and cameras, to record images of pupils this includes when on field trips. Images can only be taken on school cameras.
- Permission to use images of pupils is sought each year through the registration/re-registration form.
- Permission to use images of all staff who work at the school is sought on induction.
- Pupils' names will not be published alongside their image and vice-versa on-line.

Video Conferencing and the use of Webcams

Video conferencing has offered valuable educational and social opportunities to connect with other schools. Webcams in school are only ever used for specific learning purposes and all images recorded and transmitted are the responsibility of the teacher using them.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use during non-contact time with pupils.
- The school discourages members of staff contacting a parent/carer using their personal device.
- The school is not responsible for the loss damage or theft of any personal mobile device.

- The sending of inappropriate text messages between members of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and PDA for off-site visits and trips, only these devices should be used.

Writing and Reviewing this Policy

Staff have been involved in the making of the Policy for E-safety through training sessions and on-going consultation. This policy will be reviewed every 24 months (or sooner in relation to advances in ICT or if breaches have been detected) and consideration given to the implications for future whole school development planning.

A sub-committee of the Board of Governors will monitor and evaluate the effectiveness of this policy as part of a timetabled, on-going process.

This policy was updated on 5th January 2016.

Appendix 1

Acceptable Use Agreement/E-Safety Rules (Staff and Governors)

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 policy is designed to ensure that all staff and Governors are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I will only use the school's e-mail/internet/and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or C2k.
- I will ensure that all electronic communications with 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 have been advised not to give out my own personal details such as mobile phone number and personal e-mail address to parents/carers.
- I will use the approved, secure C2k e-mail system for any school business.
- I will ensure that school personal data is kept secure and is used appropriately, whether in school taken off the school premises or accessed remotely
- I will not install any hardware or software without the permission of the ICT co-ordinator.
- 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.
- I will support the school approach to on-line safety and not deliberately share or upload any images, video or text that could upset or offend any member of the school community.
- 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 on-line activity, both in school and outside school will not bring Kilronan School or my professional role into disrepute.
- I will support and promote the school's E-safety and Child Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies in the context of school.
- I understand the sanctions related to breaches of the above.

User Signature

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

Full Name (Printed) _____

Signature _____

Date _____

Kilronan School E-Safety Protocols
Staff

Please be advised as follows:

1. On social media, do not disclose your place of work as Kilronan School.
2. On Personal Social Media do not make any direct reference to your class or the school name.
3. Do not make friends with parents of pupils.
4. Do not make friends with past pupils.
5. Keep your profile settings set to friends only. If the settings are public then everyone can see what you post.
6. Remember that anything posted on your page is a reflection on you and your professionalism at work, and could be a reflection on the school.
7. Future or potential employers may nowadays look at you social media profile/page to view how you conduct yourself.
8. Do not be offended if other staff do not accept you as a friend on social media. If we are not friends in school or socially outside of school with everyone we work with, why do we need to be friends on such sites? We are all work colleagues. There is a difference. Do not take offence.

   NB. Today you have been given this information. It is your decision whether you follow the advice given. However, as a school, if there is any issue in the future regarding any of these points then Kilronan as a school will not accept any responsibility.

   We thank you for your professionalism and trust you will make choices which safeguard both you and the pupils.

Appendix 3

Trifold leaflet