Learning, growing and achieving together

KILRONAN
SCHOOL

E-Safety and Acceptable Use of the Internet and Digital Technologies Policy

Re-issue Date: May 2023

Review Date: May 2025

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

United Nations Convention on the Rights of the Child (UNCRC):

All children have the right to:

- Freedom of expression. They must be free to express their thought and opinions and to access all kinds of information, as long as it is within the law (Article 13).
- Privacy. The law should protect the child's private family and home life, including protecting children from unlawful attacks that harm their reputation (Article 16).
- Reliable information from a variety of sources and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them. (Article 17).
- An education which will be differentiated to meet their individual needs (RRS team 2015). Every child has the right to an education (Article 28).

CONTENTS

VISION

At Kilronan School we aim to provide a happy, safe and stimulating learning environment where pupils are motivated to achieve, feel valued and are respected as individuals. We believe our inclusive approach meets the needs of each pupil and empowers them to reach their full potential through experience of and participation in all aspects of the curriculum.

We are committed to:

- Putting pupils first
- Providing a welcoming, dynamic and supportive learning and teaching environment.
- Delivering the Pre-School/ NI Curriculum, School Leavers Programme, through an individualised and child centered approach.
- Ensuring that the highest standards of Pastoral Care, Safeguarding and Child Protection are in place.
- Promoting and sustaining good behaviour.
- Treating everyone with dignity and respect.
- Continuing to foster and develop effective home/school links.
- Working together as a team for the benefit of each pupil.
- Working collaboratively with Allied Health Professionals and other agencies to ensure the needs of pupils are met.
- Developing and maintaining close links with other schools and the local community for the mutual benefit of all.
- Giving all staff opportunities for appropriate continuing professional development.
- Embracing new opportunities and innovative approaches to meet the changing needs of the pupils and the school.

Kilronan Special School E-Safety & Acceptable Use of the Internet & Digital Technologies Policy

1. Introduction

1.1 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.

1.2 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.

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups associated with Kilronan School. It should be noted all stakeholders hold a shared responsibility with the common aim of protecting all pupils.

2.1 Board of Governors

Have a responsibility 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(s) for Safeguarding and Child Protection.

2.2 The Principal

Has a responsibility 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 concern.
- Agree with BoG any appropriate pastoral or disciplinary measures to be taken.

2.3 Safeguarding - Designated and Deputy Designated Teachers

Have a responsibility to:

Maintain current and up to date training in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

2.4 Teaching and Classroom Staff

Have a responsibility to:

- Maintain an up-to-date awareness of online safety matters and Kilronan's online safety policy and practice.
- Read, understand and sign the staff acceptable use policy/agreement.
- Report any suspected misuse or problem to the *Principal/Designated/ Deputy Safeguarding* Teacher(s) for investigation.
- Ensure all digital communications with students/pupils/parents/guardians is kept on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Students/pupils understand and follow the Online Safety Policy and acceptable use policies.
- Monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

3. Monitoring

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

4. Breaches

4.1 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.

5. Incident Reporting

5.1 Any security breaches or attempts and any unauthorized 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 Deehan (Principal) or Miss Holmes (Vice Principal).

6. E-mail

6.1 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 Deehan and Miss Holmes) if they receive an offensive e-mail.

7. E-Safety

7.1 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 have access to 'Kilronan School E-Safety Protocols' (Appendix 2) produced by the Designated Teacher and Deputy Designated Teachers' for Safeguarding and Child Protection.
- Members of the ICT team (Mrs J Ambrose and the Designated Safeguarding teacher (Mrs Shaw) undertake regular e safety training organized by C2k and the UK Safer Internet Centre.
- Safer Internet Day is acknowledged annually (usually in February) with each class marking the occasion and raising awareness, with a whole school approach.
- 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 Coordinator.
- 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.

8. Social Net-working Sites

8.1 It is important to recognise that there are issues regarding the appropriateness of some content and contact in relation to social net-working sites. Staff are therefore encouraged to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. Images once on-line can never be removed.

- Access to social net-working sites using C2k computers is forbidden.
- Access to social net-working sites using personal mobile phones during working hours is not permitted.
- Staff should not discuss any school related business on social net-working sites.
- Images of pupils or the school environment are not permitted to be uploaded on to social net-working sites apart from Kilronan's Facebook page and the 'closed' friends and family page. Only Mrs Shaw, Miss Adams, Mrs Deehan, Miss Holmes and Miss Young have access to update these pages.
- Images of staff are not to be uploaded on to social net-working sites without the permission of the staff member/s involved.

9. Parental Involvement

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

- Parents/guardians are asked to read through the e-safety trifold leaflet (Appendix 3).
- Parents/guardians are required to decide as to whether they consent to images of their son/daughter being taken for use in school/website/Facebook page/media.

- Parents will be made aware of the Swiggle search engine and encouraged to use it at home for young people who browse the internet independently. Swiggle is an ad free and child friendly search engine which aims to keep children safe and secure when online.
- Through the Registration/Re-Registration form, parents/guardians 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, Seesaw App and Facebook page.

10. Safe use of ICT Equipment

(Including Portable and Mobile ICT Equipment and Removable Media)

10.1 School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- ICT equipment issued to staff is recorded and serial numbers form part of the school's inventory.
- All ICT equipment is kept physically secure.
- It is imperative that you save your data on a frequent basis to the school's network drive.
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment, resignation or transfer, all ICT equipment must be returned to School. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

10.2 Portable and Mobile ICT Equipment

This section covers such items as laptops, iPads, memory sticks and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data:

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on the school network and not kept solely on the device. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. All teacher iPads are to be given to ICT Coordinator during school holidays (The Leadership Team must be informed of any exceptions, which have been granted by the Principal/VP).
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades (approximately every six weeks).
- The installation of any applications or software packages must be authorised by the ICT support team fully licensed and only carried out by your ICT support.
- Staff who have ceased employment must return to the ICT coordinator all portable and mobile ICT equipment, unlocked, cleared of personal information and ready for use.
-

11. 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/ Mrs J Ambrose) when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

12. 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/guardians 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' full names will not be published alongside their image and vice-versa on-line.

13. Video Conferencing and the use of Webcams

13.1 Video conferencing (such as Microsoft Team and Zoom) has offered valuable educational and social opportunities to connect with others (especially during the Lockdown and the Covid Pandemic). Webcams in school are only ever used for specific learning purposes and all images recorded and transmitted are the responsibility of the staff using them.

14. 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. Mobile phones are not permitted for use during pupil contact time
- The school discourages members of staff contacting a parent/guardian 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, iPads, laptops and PDA for off-site visits and trips, only these devices should be used

15. Writing and Reviewing this Policy

15.1 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.

16. Current Legislation

16.1 Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individual rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

16.2 Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

16.3 Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith or to stir up religious hatred by displaying, publishing, or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality, or ethnic background.

16.4 Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of *"Children and Families: Safer from Sexual Crime"* document as part of their child protections packs.

16.5 Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

16.6 The Computer Misuse Act 1990 (sections 1-3)

Regardless of an individual's motivation, the Act makes is a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)

16.7 Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

16.8 Copyright Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text music sound film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a license associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a license before you copy or use someone else's material. It is also illegal to adapt or use software without a license or in ways prohibited by the terms of the software license.

16.9 Public Order Act 1986 (sections 17-29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

16.10 Protection of Children Act 1978 (section 1)

It is an offence to take, permit to be taken, make, possess show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

16.11 Obscene Publications Act 1959 and 1964

Publishing an "obscene article" is a criminal offence. Publishing includes electronic transmission.

16.12 Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

16.13 Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga 19980029 en 1

16.14 The Freedom of Information Act 200

http://www.ico.gov.uk/for organisations/freedom of information guide.aspx

MONITORING AND REVIEW

This policy will be monitored appropriately and reviewed for revision as necessary.

Signed: **(Chairperson of Board of Governors)**

Signed: Sharlene Deehan **(Principal)**

Date: 18th May 2023

Version	**Date**	**Revision Author**	**Summary of Changes**
2	April 2023	Policy Subcommittee	Format to include vision and content page.

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/guardians.
- 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 coordinator.
- 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____

Appendix 2

Kilronan School E-Safety Protocols

Staff

Please be advised as follows:

- On social media, do not disclose your place of work as Kilronan School.
- On Personal social media do not make any direct reference to your class or the school name.
- Do not make friends with parents of pupils.
- Do not make friends with past pupils.
- Keep your profile settings set to friends only. If the settings are public then everyone can see what you post.
- 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.
- Future or potential employers may look at your social media profile/page to view how you conduct yourself.
- 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

Kilronan Pupil Acceptable Digital Technologies Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse.
- that pupils in return for good access to digital technologies to enhance their learning will agree to be responsible users.

This is how I stay safe when I use computers/ iPads/ the internet:

- I will gain permission from the teacher or suitable adult when I wish to use the computers/tablets (e.g., iPads).
- I will only use activities that a teacher or suitable adult has given permission for me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult when needed.
- I will tell a teacher or suitable adult if I view something upsetting or worrying.
- I will not share personal information about myself or others when on-line, when in school or at home (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I know that if I break the rules, I may not be allowed to use a computer/tablet.

- If using social media, I will not request staff to my ‘friend’s’ list and not behave in a way that may bring Kilronan School’s reputation into disrepute.

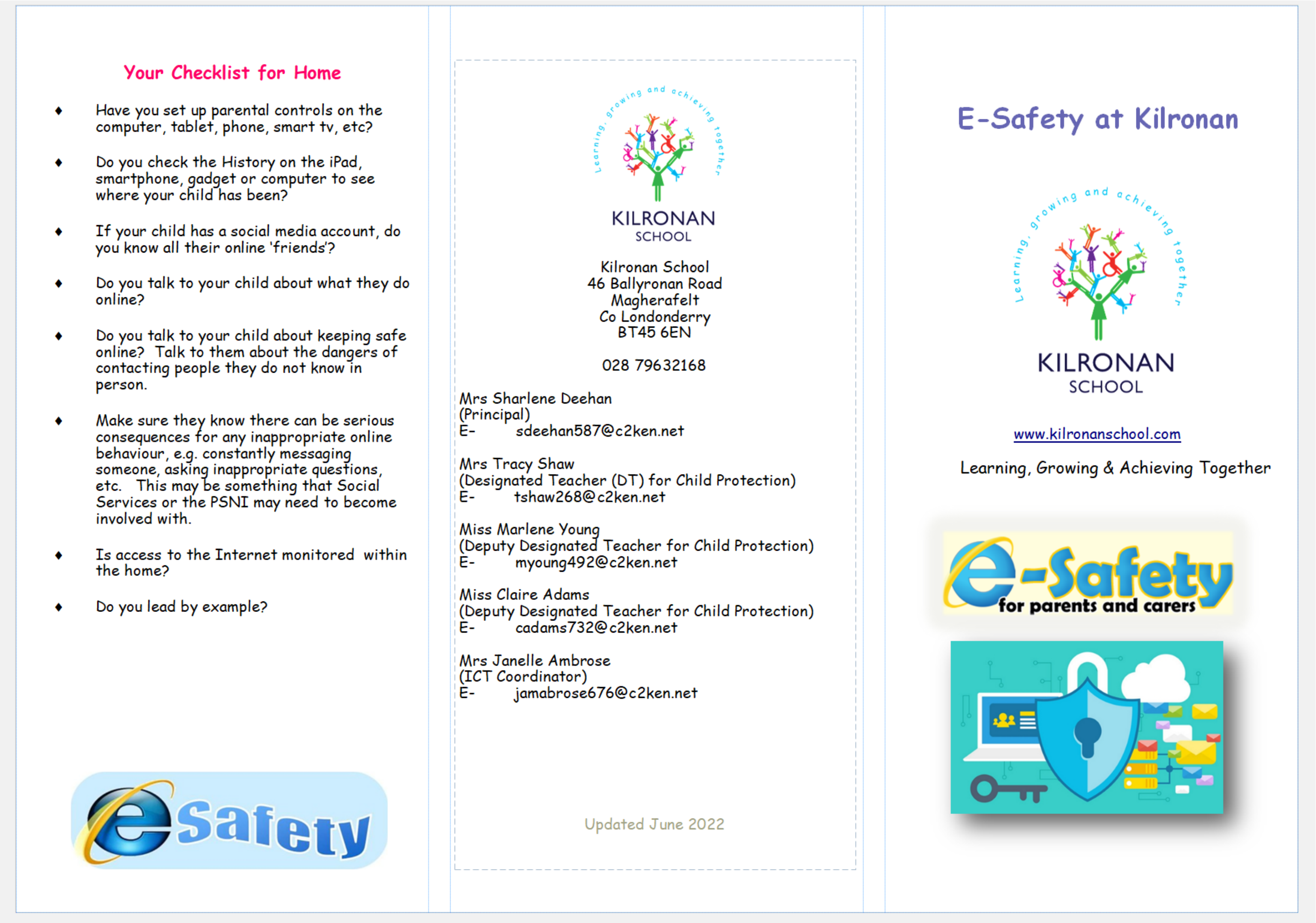
Signed (Pupil)____

Date____

Signed (Parent)_______________________________________

Date____

Appendix 4, Side A.



Your Checklist for Home

- Have you set up parental controls on the computer, tablet, phone, smart tv, etc?
- Do you check the History on the iPad, smartphone, gadget or computer to see where your child has been?
- If your child has a social media account, do you know all their online 'friends'?
- Do you talk to your child about what they do online?
- Do you talk to your child about keeping safe online? Talk to them about the dangers of contacting people they do not know in person.
- Make sure they know there can be serious consequences for any inappropriate online behaviour, e.g. constantly messaging someone, asking inappropriate questions, etc. This may be something that Social Services or the PSNI may need to become involved with.
- Is access to the Internet monitored within the home?
- Do you lead by example?

eSafety

KILRONAN
SCHOOL

Kilronan School
46 Ballyronan Road
Magherafelt
Co Londonderry
BT45 6EN

028 79632168

Mrs Sharlene Deehan
(Principal)
E- sdeehan587@c2ken.net

Mrs Tracy Shaw
(Designated Teacher (DT) for Child Protection)
E- tshaw268@c2ken.net

Miss Marlene Young
(Deputy Designated Teacher for Child Protection)
E- myoung492@c2ken.net

Miss Claire Adams
(Deputy Designated Teacher for Child Protection)
E- cadams732@c2ken.net

Mrs Janelle Ambrose
(ICT Coordinator)
E- jamabrose676@c2ken.net

Updated June 2022

E-Safety at Kilronan

Learning, growing and achieving together

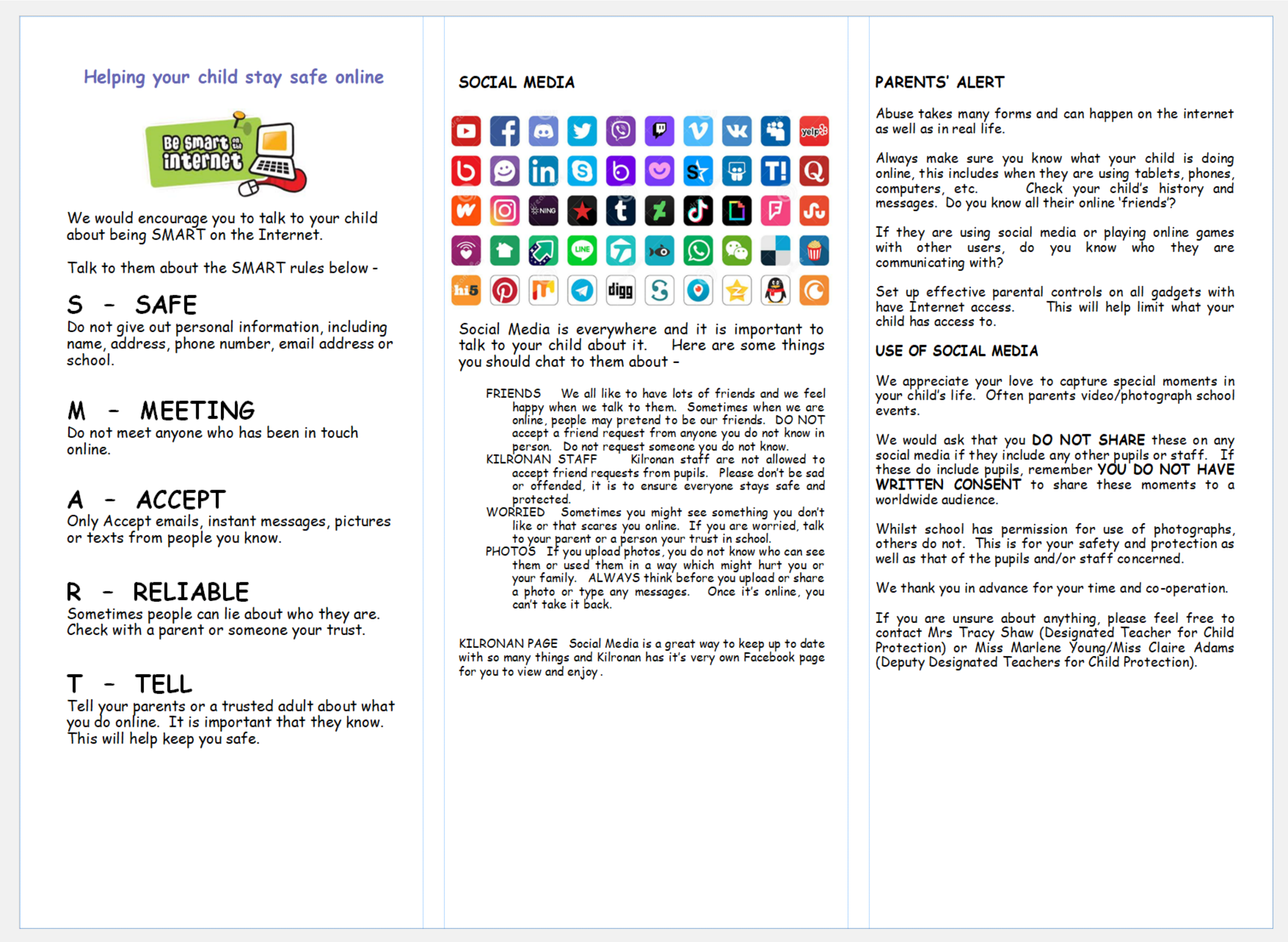
KILRONAN
SCHOOL

www.kilronanschool.com

Learning, Growing & Achieving Together

e-Safety for parents and carers

Appendix 4, Side A.



Helping your child stay safe online

Be smart on the internet

We would encourage you to talk to your child about being SMART on the Internet.

Talk to them about the SMART rules below -

S - SAFE

Do not give out personal information, including name, address, phone number, email address or school.

M - MEETING

Do not meet anyone who has been in touch online.

A - ACCEPT

Only Accept emails, instant messages, pictures or texts from people you know.

R - RELIABLE

Sometimes people can lie about who they are. Check with a parent or someone your trust.

T - TELL

Tell your parents or a trusted adult about what you do online. It is important that they know. This will help keep you safe.

SOCIAL MEDIA

Social Media is everywhere and it is important to talk to your child about it. Here are some things you should chat to them about -

FRIENDS We all like to have lots of friends and we feel happy when we talk to them. Sometimes when we are online, people may pretend to be our friends. DO NOT accept a friend request from anyone you do not know in person. Do not request someone you do not know.

KILRONAN STAFF Kilronan staff are not allowed to accept friend requests from pupils. Please don't be sad or offended, it is to ensure everyone stays safe and protected.

WORRIED Sometimes you might see something you don't like or that scares you online. If you are worried, talk to your parent or a person your trust in school.

PHOTOS If you upload photos, you do not know who can see them or used them in a way which might hurt you or your family. ALWAYS think before you upload or share a photo or type any messages. Once it's online, you can't take it back.

KILRONAN PAGE Social Media is a great way to keep up to date with so many things and Kilronan has it's very own Facebook page for you to view and enjoy.

PARENTS' ALERT

Abuse takes many forms and can happen on the internet as well as in real life.

Always make sure you know what your child is doing online, this includes when they are using tablets, phones, computers, etc. Check your child's history and messages. Do you know all their online 'friends'?

If they are using social media or playing online games with other users, do you know who they are communicating with?

Set up effective parental controls on all gadgets with have Internet access. This will help limit what your child has access to.

USE OF SOCIAL MEDIA

We appreciate your love to capture special moments in your child's life. Often parents video/photograph school events.

We would ask that you **DO NOT SHARE** these on any social media if they include any other pupils or staff. If these do include pupils, remember **YOU DO NOT HAVE WRITTEN CONSENT** to share these moments to a worldwide audience.

Whilst school has permission for use of photographs, others do not. This is for your safety and protection as well as that of the pupils and/or staff concerned.

We thank you in advance for your time and co-operation.

If you are unsure about anything, please feel free to contact Mrs Tracy Shaw (Designated Teacher for Child Protection) or Miss Marlene Young/Miss Claire Adams (Deputy Designated Teachers for Child Protection).