



ICT Acceptable Use and Online Safety Policy

Reviewed April 2021

KILMORIE
PRIMARY SCHOOL

Written by Emanuela Brahamsha
Agreed by Governing Body June 2021
To be reviewed April 2022

Introduction and Aims

At Kilmorie we believe that ICT is central to all aspects of learning; for adults and children in both the school and the wider community. Provision should reflect the rapid developments in technology.

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to equip our young people with the skills to access lifelong learning and employment.

All children, whatever their needs, will have access to a range of up to date technologies in both the suite and classrooms. ICT is a life skill and should not be taught in isolation.

The computer science curriculum covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Kilmorie Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach... Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks'
(Becta Safeguarding Children Online Feb 2009)

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Relevant Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [teaching online safety](#), [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and

deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the [National Curriculum computing programmes of study](#).

Roles and Responsibilities

At Kilmorie we take a whole school approach to online safety and expect that all members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures. This includes vigilance when children are accessing the internet at school to ensure that they do not access inappropriate websites.

The specific roles and responsibilities include:

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of the school's Designated Safeguarding Lead and deputies are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

The ICT manager

The ICT manager is managed by the School Business Manager and is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a [weekly/fortnightly/monthly] basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

All staff, contactors, agency staff and volunteers

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the 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 on the school website
- procedures in the event of misuse of technology by any member of the school community (see appendices)
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school (see appendix 1 for staff acceptable use agreement).

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Read, understand and adhere to the terms of acceptable use of the school's internet and social media (Appendix 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - [UK Safer Internet Centre](#)

Hot topics - [Childnet International](#)

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. The children will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. We will also provide workshops and signpost parents to information sessions run by third parties, such as the local authority.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour Policy and Anti-Bullying Policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying during computing and PSHE lessons and the issue will be addressed in assemblies.

All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school will also send information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the school's COVID-19 risk assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

ACCEPTABLE USE:

Managing Internet Access

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

When children access internet resources for work set by school for work in school or at home:

- Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.

- Raw image searches are discouraged when working with pupils.
- Specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
- Our internet access is controlled through the LGFL web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to an ICT leader, technician or member of SLT.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

E-mail

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school, between schools or international. We recognise that pupils need to understand how to style an email in relation to their age.

- Pupils are introduced to email as part of the Computer Science Scheme of Work.
- The school gives staff their own email account, which they must use for all school business. They must not use a personal email account for any school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. Staff will be encouraged to develop and appropriate work life balance when responding to emails, especially if communication is taking place between staff and parents.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail. All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone. Staff must inform a member of SLT if they receive an offensive e-mail.

Passwords:

All users will be informed not to share passwords or information with others and not to login as another user at any time. Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.

All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their passwords private.

Pupils using mobile devices in school

Year 5 and Year 6 pupils may bring mobile phones into school once their parents have informed the school. All phones must be handed to into the school office before lining up for class and collected at the end of the day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy. This may result in the confiscation of their device.

COVID amendment: Devices will be handed into the class/bubble teacher at the beginning of the day and collected at the end of the day.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school

If staff have any concerns over the security of their device, they must seek advice from the School Business Manager.

Work devices must be used solely for work activities.

Social networking and personal publishing

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Pupils and parents will be advised never to give out personal details of any kind which may identify them or their location.

Remote Learning

Online safety is even more of a priority for schools and families during the coronavirus lockdown. Away from school and with time on their hands, children are at a greater risk than ever from online dangers. We will continue to play a key role in reinforcing the online safety message with the children and their families, providing reminders, advice and helpful resources.

Working in Partnership with Parents

Parents/carers are asked to read through and sign acceptable use of ICT agreements on behalf of their child on admission to school (see appendix 1).

- Read, understand and adhere to the terms of acceptable use of the school's internet and social media (Appendix 2).
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website).
- A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use.
- Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

Data protection

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

Responding to e-safety incidents/complaints

Where a pupil misuses the school's ICT systems or internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

As a school we 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. The school cannot accept liability for material accessed, or any consequences of Internet access.

Complaints relating to e-safety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Head teacher.

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with SLT any issue of safety that concerns them. The DSL, Headteacher or class teacher will log behaviour and safeguarding issues related to online safety.

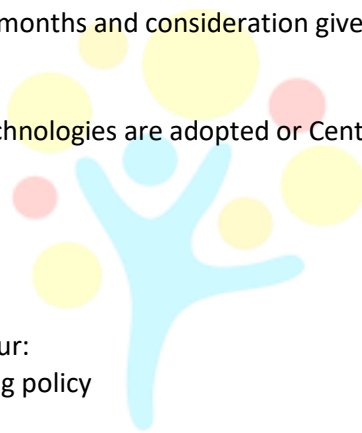
This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff code of conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- GDPR policy



KILMORIE
PRIMARY SCHOOL

**Appendix 1: ICT Acceptable Use Policy for pupils:
Agreement / eSafety Rules**

- I will take care when using the school IT equipment and use it properly
- I will only share my user name and password with trusted adults
- I will tell an adult if I see anything that upsets me
- I will make sure that when I blog I am responsible, polite and sensible
- I will use a safe name and not my real name on the internet
- I know I am only allowed to go on the internet if my teacher has given me permission
- I will only take a photograph or video of someone if they say it is alright
- Any messages I send will be polite
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computer or internet for a while, even if it was done outside school

Parent/ Carer signature

We have discussed this and (childs name)

agrees to follow the eSafety rules and to support the safe use of ICT at Kilmorie Primary
School

Parent / Carer Name (PRINT)

Parent / Carer (Signature)

Class Date.....

Appendix 2

Acceptable use of the internet: agreement for parents and carers

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Our official Twitter feed
- Email/text to parents
- Our website
- Microsoft Teams
- Seesaw

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's concerns and complaints procedure

I will not:

- Use private groups (e.g. WhatsApp), the school's Facebook page or Twitter account, or personal social media to bring the school into disrepute
- Upload or share photos or videos on social media of any child other than my own, without the express permission of the other children's parents/carers

Slander or harassment of the school, other parents or staff, online or otherwise will be taken seriously and reported to the relevant authorities.

Appendix 3:



Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

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

- I will only use the school's email / Internet / Network/ Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will not email documents giving details of pupils unless on a secure system such as Egress.
- I will ensure that personal data (such as data held on ScholarPack or Access Education) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. USB sticks containing data must be encrypted. These are supplied by school.
- I will not use or install any hardware or software without permission from the ICT technician.
- 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 with school devices, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or head teacher. I understand I cannot use my mobile phone to take photos of children
- 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 by the Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature Date

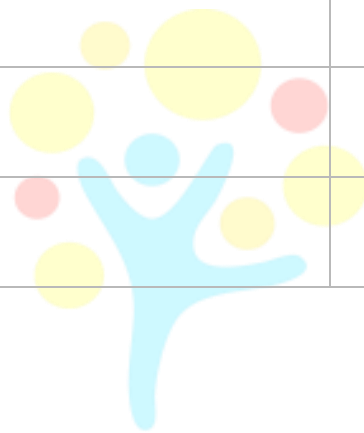
Full Name (printed)

Job title:

Appendix 4:

ONLINE SAFETY INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident



KILMORIE
PRIMARY SCHOOL