Kilmorie Primary School

Online Safety Policy

This policy was agreed by the governing body on: (and supersedes all previous policies relating to this area)	
Signed: Chair of Governors:	
Implemented:	September 2025
Reviewed:	July2025
Review date:	
Author:	Dennis Irwin Headteacher

Contents

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Our approach to online safety is based on addressing the following categories of risk:

The 4 key categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

1. 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 in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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, Relationships, health and Sex Education Policy and the Computing curriculum.

Online Safety Act July 25: As of 25 July 2025, platforms have a legal duty to protect children online. Platforms are now required to use highly effective age assurance to prevent children from accessing pornography, or content which encourages self-harm, suicide or eating disorder content.

Platforms must also prevent children from accessing other harmful and age-inappropriate content such as bullying, hateful content and content which encourages dangerous stunts or ingesting dangerous substances. Platforms must also provide parents and children with clear and accessible ways to report problems online when they do arise.

A full explanation of how the Act works, and how it protects different groups is available in the Online Safety Act explainer.

Ofcom has also created a guide for parents.

2. Roles and responsibilities

2.1 The governing body

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

The governing body will ensure that the school checks that all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure the school provides regular online safety updates for staff (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will be invited to regular meetings with appropriate staff (DSL/ICT Lead Officer/Inclusion Lead) to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body will review the school's approach to children being taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is the designated Online Safety Governor.

All governors will:

- Ensure 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)
- Ensure that online safety is a running and interrelated them while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

2.2 The Headteacher

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

2.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our safeguarding and child protection policy.

The Inclusion lead / DSL take joint 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT technician and Wavenet to make sure the appropriate systems and

processes are in place

- Working with the Headteacher, ICT technician, and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's safeguarding and child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged on CPOMs 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 with ICT lead officer (appendix 5) - a self-audit for staff on online safety training needs)
- 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
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

2.4 The ICT Lead Officer (in conjunction with Wavenet)

The ICT Lead Officer 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 frequently and when applicable.
- Blocking access to potentially inappropriate and dangerous material and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported to the DSL

This list is not intended to be exhaustive.

2.5 All staff and volunteers

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 (appendix 1)
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and

being aware of how to report any incidents of those systems or processes failing by [insert school specific action here]
- Working with the DSL to ensure that any online safety incidents are on CPOMS 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
- Responding to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

2.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy

Parents and carers should be aware of the children's Acceptable Use Policy as displayed on the school website. Children will read and agree to this policy within the first week of the Autumn term. New children will be asked to read and agree within their first week of joining. (Appendix 1)

- Parents/carers 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

Parent resource sheet – Childnet International

2.7 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 2).

3. Educating pupils about online safety

It is important that schools establish a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.
Our teaching focuses on underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app.
The following subjects have the clearest online safety links:

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

However, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Pupils will be taught about online safety as part of the curriculum. In **Key Stage 1**, pupils

In **Key Stage 1 (KS1)**, 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 (KS2)**, 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

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, workshops and in information via our website or virtual learning environment (Teams). This policy will also be shared with parents.

Online safety will also be covered during parents' evenings where relevant.
The school will let parents/carers know via newsletters, leaflets, a monthly online safety newsletter parent workshops and the school website, the following:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Online Safety Lead or Headteacher or the DSL.

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

5. Cyber-bullying

5.1 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and antibullying policy.)

5.2 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 12 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected. Additionally, Workshops for parents are held at least annually

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, the DSL will work with external services where deemed necessary to do so.

5.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher (as set out in the behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL / Inclusion Lead
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / Inclusion Lead to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not

delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:
- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

5.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft Copilot.

Kilmorie Primary School recognises that AI has many uses to help pupils learn but may also have the potential for potential harm e.g. it can be to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Kilmorie will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

6. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 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.

ICT Lead Officer will monitor, at regular intervals, websites visited, and searches done by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

7.1 Appropriate filtering and monitoring

Keeping Children Safe in Education (2023) obliges schools to ensure that appropriate filtering and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

7.2 Monitoring arrangements

- The DSL (and deputies) log behaviour and safeguarding issues related to online safety All incidents are recorded and monitored using CPOMs and SENSO (LGFL monitoring platform)
- This policy will be reviewed every year by the online safety leads (DSL & Inclusion Lead in conjunction with the Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Kilmorie Primary we have decided that option 3 is appropriate in addition to options 1 and 2 because it monitors to a higher level. London Grid for Learning provides a technology-based monitoring system that actively monitors use through keywords and other indicators across devices. This system is particularly effective at drawing attention to concerning behaviours, communications or access.

7. Pupils using mobile devices in school

Pupils in Year 5 and Year 6 should not bring smart phones to school. However, they may bring? non smart phones into school, but are not permitted to use them during:

- At anytime on school grounds
- Clubs before or after school, or any other activities organised by the school

Any use of **school** mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Mobile phones must be turned off once on the school grounds and handed in to the child's class teacher at the start of the day 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, which may result in the confiscation of their device.

8. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping a laptop device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol). Mobile devices should be protected with a minimum of 4 digit code or biometrics.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates
- 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.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

Work devices should only be used for work activities.

9. How the school will respond to issues of misuse

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE/RSHE).

Kilmorie Primary commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The new DfE guidance Behaviour in Schools, advice for Headteacher and school staff July 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online safety incidents involving their children, and where applicable, the police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies; behaviour, anti-bullying, safeguarding policy. 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 / 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police where applicable.

10. Staff, pupils' and parents' social media presence

Social Media Use in the School Community

- Social media is widely used and acknowledged by the school.
- All users must follow the school's Acceptable Use Policies and behave respectfully online, as they would in person.
- Inappropriate posts (bullying, rude, illegal, or damaging to the school/staff) are not acceptable—this includes private groups and chats-applies to both public and private platforms (e.g. WhatsApp groups).
- Concerns should be raised privately with the school, not on social media. Use the official complaints procedure if needed.
- Public complaints can harm staff morale, upset the community, and damage the school's reputation.

Age Restrictions & Online Safety

- Most platforms are 13+ (WhatsApp is 16+); underage use is discouraged.
- Parents should respect age ratings and avoid encouraging underage access.
- Online safety lessons cover respectful behavior, reporting abuse, and digital citizenship.
- Children learn most from adult behavior online—parents are key role models.

Parental Support & Resources

- Talk to children about their apps, games, and online habits (who, when, how long).
- Avoid late-night/bedroom use to support sleep and learning.
- Use tools like:
- Digital Family Agreement
- Top Tips for Parents
- Online Safety Newsletter
- parentsafe.lgfl.net
- Children's Commission Digital 5 A Day

Communication & Boundaries

- **Email** is the official communication channel between parents and school.
-

Staff & Pupil Boundaries

- Pupils must not friend/follow or message staff, governors, or volunteers.
- Staff must not follow pupil accounts.
- Staff should:
- Use strict privacy settings.
- Avoid discussing school matters online.
- Ensure personal posts don't reflect poorly on the school or profession.
-

Consequences & Policies

- Misuse of social media can lead to serious consequences—333 teachers faced Prohibition Orders

in 6 years due to online misconduct.

- All social media activity is subject to:
  - **Acceptable Use Policies (Appendices 1–3)**
  - **School's Data Protection Policy**

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). They will also complete a training needs audit as required (appendix 5).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding and child protection policy.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures

- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: acceptable use agreements: Kilmorie KS1 pupils

LGfL SafeguardED

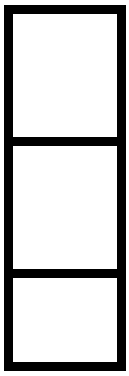
Acceptable Use Policy (AUP) for KS1 PUPILS

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:	✓
1. I only **USE** devices or apps, sites or games if I am allowed to.	
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared or confused.	
3. I look out for my **FRIENDS** and tell someone if they need help.	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult.	
5. I **KNOW** that online people aren't always who they say they are and things I read or see are not always **TRUE.**	
6. Anything I do online can be shared and might stay online **FOREVER.**	
7. I don't keep **SECRETS** 🚫 unless they are a nice surprise.	
8. I don't have to do **DARES OR CHALLENGES** ❌, even if someone tells me I must. Sometimes these can be dangerous.	

9. I don't change **CLOTHES** or get undressed in front of a camera.

10. I always check before **SHARING** my personal information or other people's stories, videos and photos.

11. I am **KIND** and polite to everyone.



Appendix 1: Acceptable use agreements: Kilmorie KS2 pupils

LGfL SafeguardED

Acceptable Use Policy (AUP) for KS2 PUPILS

1. ***I learn online*** – I use school internet, devices and logins for school and homework, to learn and have fun. School can see what I am doing to keep me safe, even when at home.
2. ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use devices, apps, sites and games if and when I am allowed to. If not sure, I will ask.
4. ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things, remembering my 'Digital 5 A Day'.
5. ***I am a good friend online*** – I won't share or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am not a bully*** – I know just calling something fun or banter doesn't stop it may be hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments, images or videos and if I see it happening, I will tell my trusted adults.
7. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
8. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
9. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
10. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
11. ***If I make a mistake, I don't try to hide it but ask for help.***

12. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about. I check with a trusted adult before I chat with anyone for the first time, even if they are a 'chatbot'.
13. ***I know online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
15. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
16. ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
17. ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I don't create artificial images, videos or deepfakes of others without consent. I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
18. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
19. ***I can say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
20. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
21. ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
22. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
23. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
24. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and age restrictions. I follow rules, block bullies and report bad behaviour, at home and at school.
25. ***I am part of a community*** – I do not say mean things, make fun of anyone or exclude them because they are different. If I see anyone doing this, I tell a trusted adult and/or report it. I talk to others online how I would like to be spoken to.
26. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
27. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see, and I know which sites to trust, and how to double check information I come across. I will not copy anything without permission. If I am not sure I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:

At school that might mean _____all staff_____

Outside school, my trusted adults are_____parents/carers___

I know I can also get in touch with Childline

Appendix 2: Acceptable use agreement Parents

Background

The use of technology is an essential part of all of our lives. At Kilmorie Primary School we take our responsibilities for supporting your child to develop skills in using technology very seriously, and their safety and wellbeing are our utmost priority to us.

We ask all children, young people and adults involved in the life of Kilmorie Primary School to read and sign an Acceptable Use* Policy (AUP) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an AUP which is available here.

We tell your children that they should not behave any differently when they are out of school or using their own device or on a home network. What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

What am I agreeing to?

1. I understand Kilmorie Primary School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including through behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.

3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to over block or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
5. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school is subject to filtering and monitoring. More detail of this can be found in our online safety policy.
6. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
8. I will support my child to follow the school's policy regarding bringing devices (mobile phones, tablets, Smart watches and glasses etc.)
9. I understand that my child might be contacted online on Microsoft Teams which are approved for school by class teachers, form tutor, head of year, and only about their learning, wellbeing or behaviour.
10. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

11. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age (for nearly every social media platform, this means under 13 years old).
12. When I visit the school premises, I will keep any online technology in my pocket wherever possible.
13. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information). The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
14. I will not covertly film or make recordings of any interactions with pupils or adults in schools. If I wish to make any recording, we request you to please speak to the head teacher or the DSL.
15. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety and refer to parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screentime and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.
16. Research tells us that the majority of children are now accessing artificial intelligence in some form, which is available for free on most mainstream apps and social media platforms. There are some significant risks involved with this including talking to chatbots, and the use of nudifying apps and image creators to create inappropriate and illegal images/videos I will talk to my child about these risks. Find out more at parentsafe.lgfl.net
17. I understand that my child needs a safe and appropriate place to do home learning, whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
18. If my child has an online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered/safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.

19. I understand that whilst home networks are much less secure than school ones, I can apply safety settings to my home internet and to various devices, operating systems, consoles, apps and games. Find out more at parentsafe.lgfl.net
20. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content. [Previous sentence best suited to primary parents] I can also set up SafeSearch to filter explicit content from searches.
21. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my child, role model healthy behaviours and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
22. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules.

23 I can find out more about online safety at Kilmorie Primary School by reading the full Online Safety Policy here and can talk to the class teacher, DSL or the Head teacher if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

Appendix 3: Acceptable use agreement Staff, Governors and Volunteers

Acceptable Use Policy (AUP) for
STAFF, GOVERNORS, VOLUNTEERS

Background

We ask everyone involved in the life of Kilmorie Primary School to agree to the Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and staff, governors and volunteers are asked to read, understand, follow and sign it when starting at the school and whenever changes are made All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy

If you have any questions about this AUP or our approach to online safety, it is your responsibility to please speak to the head teacher or the DSL.

What am I agreeing to?

1. **(This point is for staff and governors):**
   I have read and understood Kilmorie Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area.

I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.

3. I will report any behaviour which I believe may be inappropriate or concerning in any way (by adults or pupils) to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult) and make them aware of new trends and patterns that I identify.

4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media).

5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.

6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – know that 'it could happen here'! If I am unsure how to address any issues, I will seek support from the DSL.

7. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff. The same principles apply for wearable technology.

8. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.

9. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

10. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).

11. I will check with the Headteacher if I want to use any new platform or app that has not already been approved by the school, to ensure this is quality assured. This includes any generative AI apps.

12. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods. [onlinesafetyprinciples.lgfl.net]

13. I will prepare and check all online sources and classroom resources **before** using them, for accuracy and appropriateness (including ensuring adverts do not play at the beginning of videos). I will flag any concerns about "overblocking" to the DSL (such as if I cannot access teaching materials).

14. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.

15. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.

16. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.

17. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless

of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

18. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.

19. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

20. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.

21. If I already have a personal relationship to a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.

22. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policyIf I am ever not sure, I will ask first.

23. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

24. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature. I understand that any breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

25. I will only use AI platforms that have been authorised for use (including those used with pupils and to support administrative tasks), and I will ensure that any use of these platforms is transparent, responsible, appropriate, legal and ethical. I will ensure that I abide by all data protection legislation in relation to using these platforms.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.