Reedness Primary School

Acceptable Use Policy

Purpose of the Policy

This policy outlines the school's purpose in providing access to the Internet, e-mail and other communication technologies at Reedness Primary School and explains how the school seeks to educate pupils and to avoid the potential problems that unrestricted access could create.

All staff (including support staff), governors and volunteers have 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 policies.

This policy applies to pupils, staff, governors, volunteers, contractors and visitors when accessing the school network or using technology on site and for members of staff, pupils and governors when working remotely.

Roles and Responsibilities

- <u>Governing Body</u>

Oversight of policy implementation and monitoring.
Evaluate the effectiveness of filtering and safeguarding measures.

- <u>Headteacher</u>

Ensure the policy is enforced, monitored, and reviewed.
Designate online safety and data protection leads.
Ensure online safety is integrated across curriculum and staff development.

- <u>Designated Safeguarding Lead (DSL)</u>

Lead on safeguarding and child protection matters related to ICT use.
Collaborate with pastoral teams and technical services.
Respond to reports of inappropriate or unsafe use of technology.

- <u>IT Staff / Network Managers</u>

Maintain technical security systems including filtering and monitoring provision.
Report breaches or concerns to the DSL or SLT.
Ensure users are provided with secure network access.

- <u>Staff</u>

Model appropriate use of digital technology.
Ensure compliance with Staff Code of Conduct and Teachers' Standards.

Report concerns or incidents immediately.

- Pupils

Understand and follow their Acceptable Use Agreement.
Seek help when encountering inappropriate content or conduct.

- Parents and Carers

Support the school's expectations for safe and responsible use.
Reinforce appropriate online behaviours at home.

Internet Access in School

• All staff and any other adults involved in supervising children accessing the Internet, will be provided with the school ICT Acceptable Use Policy, and will have its importance explained to them.

• Our school ICT Acceptable Use Policy is available for parents on the school website.

Using the Internet to Enhance Learning Access to the Internet is a planned part of the curriculum that will enrich and extend learning activities and is integrated into schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use. Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

• access to the Internet may be by teacher demonstration

• pupils may be given a suitable web site to access using a link from their year group links page on the school website or by clicking on a link in a teacher-prepared document

• pupils may be provided with lists of relevant and suitable web sites which they may access

• older pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher; pupils will be expected to observe the Rules of Responsible Internet Use and will be informed that checks can and will be made on files and the sites they access.

Pupils accessing the Internet will be supervised by an adult, normally their teacher, at all times. They will be taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the Internet.

Using Information from the Internet

In order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it:

• pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television

• teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium)

• when copying materials from the Web, pupils will be taught to observe copyright;

Using E-mail

It is important that communications are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

• pupils may send e-mail as part of planned lessons from their school email account

• incoming and outgoing e-mail is accessed via google classroom and Gmail

• teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail

• children will have the e-mail messages they compose checked by a member of staff before sending

Maintaining the Security of the School ICT Network

Connection to the Internet significantly increases the risk that a computer or a computer network may be compromised or accessed by unauthorised persons. Schools ICT will check that virus protection is up-to-date during their maintenance visits. The IT Coordinator will keep up-to-date with ICT developments and work with the LA as Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

Users should not expect that files stored on servers or storage media are always private.

The DSL will liaise with the school's ICT provider to ensure that the correct level of filtering and monitoring is maintained.

Log in and Passwords

Children and staff must not disclose any password or login name given to anyone or allow anyone else to use a personal account.

Children and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.

Staff and children must ensure terminals, laptops or iPads are logged off (or hibernated) when left unattended.

All staff iPads and laptops will have a uniform password that is shared only with members of staff.

Adult users are expected to manage their own areas on the network where relevant. We recommend that passwords are changed regularly (Administrative staff monthly). Anyone who needs assistance in changing their password should contact the Computing Leader or

ICT technician. Teaching iPads will be used only for the purpose of teaching; no staff will access their emails via their teaching iPad for safeguarding purposes.

Ensuring Internet Access is Appropriate and Safe

The Internet is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

• our Internet access is purchased from East Riding County Council which provides a service designed for pupils including a filtering system intended to prevent access to material inappropriate for children;

• children using the Internet will normally be working during lesson time and will be supervised by an adult (usually the class teacher) at all times;

• staff will check that the sites pre-selected for pupil use are appropriate to the age of the pupils;

• staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;

• pupils will be taught to use the Internet responsibly in order to reduce the risk to themselves and others;

• the ICT co-ordinator will monitor the effectiveness of Internet access strategies;

• the ICT co-ordinator will ensure that random checks are made on files to monitor compliance with the school's ICT Acceptable Use Policy;

• the headteacher will ensure that the policy is implemented effectively;

• methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in accordance with national guidance and that provided by the LA.

Generally, the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor East Riding County Council can accept liability for the material accessed, or any consequences of this.

The most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material, responsibility for handling incidents involving children will be taken by the IT Co-ordinator

and the DSL in consultation with the Head Teacher and the pupil's class teacher. All the teaching staff will be made aware of the incident if appropriate.

• If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the Course of action the school has taken. The school aims to work with parents/carers and pupils tom resolve any issue.

• If staff or pupils discover unsuitable sites the IT co-ordinator will be informed. The IT co-ordinator will report the URL and content to the ISP and the LA; if it is thought that the material is illegal, after consultation with the ISP and LEA, the site will be referred to the Internet Watch Foundation http://www.iwf.org.uk and the police.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use that have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet by failing to follow the rules they have been taught or failing to follow the agreed search plan when undertaking their own Internet search, then sanctions consistent with our School Behaviour Policy will be applied. This will involve informing the parents/carers. Access to the Internet may also be denied for a period.

Photographs

Prior permission is sought from all parents regarding the use of images for printed publications, media, website and videos. Staff should check the relevant permission list before using images of children.

Reedness Primary School Website: www.reednessprimaryschool.co.uk

Our school website is intended to:

• provide accurate, up-to-date information about our school

• enable pupils' achievements to be published for a wide audience including pupils, parents, staff, governors, members of the local community and others

• promote the school.

All classes may provide items for publication on the school website. Class teachers will be responsible for ensuring that the content of the pupils' work is accurate, the quality of presentation is maintained and that photo permission forms are checked before uploading.

All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status.

The point of contact on the website will be the school address and telephone number. We do not publish pupils' full names or identify individuals on our web pages. Home information or individual e-mail identities will not be published.

Social Media Use

Staff Use

Maintain professionalism and appropriate boundaries at all times. Do not 'friend' or follow pupils or ex-pupils under age 18 on personal accounts. Refrain from posting images or comments that may compromise professional standing.

Pupil Use

E-Safety lessons cover safe use of social media. Use of social platforms monitored where linked to bullying or safeguarding. Reinforce the school ethos and expectations of behaviour online.

School Accounts

Management of official accounts lies with designated staff with SLT oversight. Regular moderation and communications policy in place for public engagement. No mention of individual pupils unless authorised.

E-Safety

E-Safety is recognised as an essential aspect of Computing leadership and the Head Teacher, with the support of Governors, aims to embed safe practices into the culture of the school. The overall responsibility for E-Safety has been designated to our Head Teacher working in conjunction with the Computing Lead and DSL.

The Computing Leader ensure they keep up to date with E-Safety issues and guidance through liaison with the Local Authority E-Safety Officer and through organisations such as NSPCC and The Child Exploitation and Online Protection (CEOP).

All Staff (all teachers, supply staff and teaching partners) are reminded/ updated about E-Safety matters at least once a year and usually more often, including in-depth understanding during safeguarding training.

Children are regularly informed about e-safety through planned whole school and class assemblies and as an ongoing aspect of the computing curriculum. This includes an E-Safety week in which children explore and understand cyber-bullying and discuss how to tackle it if they encounter it. Children will be taught via Age-appropriate teaching on: Cyberbullying and online abuse, Sexting and peer-on-peer abuse, Grooming, exploitation, and Prevent Duty awareness and Misinformation, fake news, and digital resilience.

Filtering and Monitoring

School uses systems in line with the DfE's Filtering and Monitoring Standards. Filtering system reviewed regularly for effectiveness and updated as needed. Monitoring software in place to flag risks and safeguard pupils. All incidents are logged digitally by the Headteacher/DSL.

All staff understand the importance of recording and reporting any breaches of the school filtering and monitoring system and have read the latest updates from KCSIE 2025 around filtering and monitoring.

Cyberbullying

Cyberbullying can be defined as the use of Information and Communications Technology (ICT) deliberately to upset someone else and may involve email, virtual learning environments, chat rooms, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites.

Through Computing lessons, assemblies and PSHE, children will be taught the SMART rules:

- SAFE Keep safe by being careful not to give out personal information online.
- MEETING Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can't be sure who you're talking to on the Internet.
- ACCEPTING Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult.
- RELIABLE Information on the internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website.
- TELL If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place or call a helpline like ChildLine on 0800 1111 in confidence.

Artificial Intelligence (AI) Use

We recognise the increasing presence of AI tools in education, creativity, productivity, and learning. Ensure AI tools are used ethically, responsibly, and in line with safeguarding and data protection laws.

Acceptable Use of AI by Pupils

Pupils must not use AI tools (e.g., chatbots, image or video generators) to engage in cheating, plagiarism, or misinformation. AI-generated content should be clearly labelled and any prompts disclosed when part of assignments. AI must not be used to replicate staff voices, create fake identities, or manipulate media in deceptive ways.

Acceptable Use of AI by Staff

Staff may use AI (e.g., lesson planning, marking support) where compliant with GDPR and safeguarding principles. Staff must verify the accuracy of AI-generated information before instruction. AI must never be used to make solely automated decisions about pupils or staff.

Safeguards and Data Protection

AI technologies must comply with UK GDPR, including having appropriate data processing agreements in place. Personal data must not be entered into AI platforms that are not approved by the school. The school will conduct Data Protection Impact Assessments (DPIAs) where high-risk AI systems are proposed.

Oversight and Monitoring

Leaders will oversee the introduction and use of AI within the school. AI tools will be included in regular safeguarding, curriculum, and IT audits. Staff and pupils must report concerns about AI misuse via safeguarding or IT channels.

Reporting and Recording Concerns

Pupils and staff report concerns to the DSL using specified procedures. All incidents logged and actioned according to the School's Safeguarding Policy via CPOMS.

Responding to Incidents of Misuse

Breaches by Pupils

Addressed through the school's Behaviour Policy. May involve parental meetings, restorative practices, or sanctions. Safeguarding or referrals to external agencies where appropriate.

Breaches by Staff

Investigated under the school's Disciplinary Policy. May result in suspension, referral to the Local Authority Designated Officer (LADO), DBS or Teaching Regulation Agency (TRA), depending on severity.

Breaches by Others (e.g., Visitors, Contractors)

Immediate removal of access or escort from premises. Further action taken where conduct is unsafe or unlawful.

References:

- **Keeping Children Safe in Education (KCSIE)** – Department for Education (DfE)
- **Working Together to Safeguard Children** – DfE
- **Education Acts 1996 & 2002** – Statutory safeguarding duties
- **UK GDPR & Data Protection Act 2018** – Requirements for personal data security
- **Prevent Duty Guidance** – To help identify and prevent radicalisation
- **Ofsted Education Inspection Framework (EIF)** – Online safety expectations
- **DfE Filtering and Monitoring Standards (2023)**

Review and Monitoring:

This policy will be reviewed annually by the Governing Body.

Date: September, 2025

Date to be reviewed: September, 2027

Approved by: Governing Body

Signed: M.Herbert

Reedness Primary School
Acceptable Use Agreement
KS2

Following these statements will help to keep myself and others safe online whilst at school and at home

- *I learn online* – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.

- *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.

- *I ask permission* – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.

- *I am creative online* – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.

- *I am a good friend online* – I won't share or say anything that 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.

- *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!

- *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.

- *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.

- *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.

- *If I make a mistake, I don't try to hide it but ask for help.*

- *I communicate and collaborate online –* with people I already know and have met in real life or that a trusted adult knows about.

- *I know new 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.
- *I never pretend to be someone else online* – it can be upsetting or even dangerous.
- *I check with a parent/carer before I meet an online friend* the first time; I never go alone.
- *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.
- *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.
- *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.
- *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.
- *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.
- *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.
- *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.
- *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).

- *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.
- *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.
- *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.
- *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 could be:

_____

Outside school, my trusted adults are:

_____

I know I can also get in touch with Childline

Signed: _____   **Date: _____**

Reedness Primary School

Acceptable Use Agreement
EYFS and KS1

My name is _____

1. I only **USE** devices or apps, sites or games if a trusted adult says so

2. I **ASK** for help if I'm stuck or not sure

3. I **TELL** a trusted adult if I'm upset, worried, scared or confused

4. I look out for my **FRIENDS** and tell someone if they need help

5. I **KNOW** people online aren't always who they say they are

6. Anything I do online can be shared and might stay online **FOREVER**

7. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to.

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

9. I always check before **SHARING** personal information

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

My trusted adults are:

_____at school

_____ at home

Reedness Primary School
Acceptable Use Agreement
for All Adults in School

Following these statements will help to keep myself and others safe online whilst at school and at home

1. I have read and understood Reedness 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. understand the sections on.

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. Smart glasses should not be worn in school.

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.

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 policy. If I am ever not sure, I will ask first.

23.   I will not use any new technology or download any apps without agreement from the headteacher.

24.   I will not use a mobile hotspot to provide internet to any device I use in school.

25.   I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies at all times, whether or not I am on site or using a school device, platform or network.

26.   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.

27.   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 here may

lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

28.   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.

Signature: _____

Name: _____

Role: _____

Date: _____

Parents:

We ask all children and adults involved at Reedness Primary School to sign an Acceptable Use Agreement 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).

Your child has signed an AUP which is available in the Acceptable Use Policy which can be found on the school website.

We tell your children that **they should not behave any differently when they are out of school or using their own device or 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:

"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."

1. I understand that Reedness 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 behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, **including during any remote learning periods.**

4. 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.

5. The impact of social media use is often felt strongly in schools, 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.

6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. 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. 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.

7. I understand that for my child to grow up safe online, they will need positive input from school and home, so I will talk to my child about online safety and support 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...

8. **I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed. When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, 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.**

9. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.

10. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children.

11. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which they have signed, and I understand that they will be subject to sanctions if they do not follow these rules.

12. I can find out more about online safety at Reedness by talking to my child's teacher 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.