



Ruardean C of E Primary School

Acceptable Use Policy

Love of Learning – Love of Life – Love of One Another

Matthew ch22 v33-40

Policy Reviewed:	Bi-Annually
By:	Resources Committee
Agreed:	04/02/2026
Next Review:	January 2028

Statement of intent

Ruardean C of E primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

1.1 Purpose

The purpose of this policy is to:

- Have robust processes in place to safeguard and protect all members of the school's community online.
- Deliver an effective approach to online safety of pupils, staff, volunteers and governors.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards practice when using technology.
- Identify clear procedures to identify, intervene and escalate an incident, where appropriate.

2.0 Implementation

The implementation of this policy is the responsibility of all teaching staff and should be overseen and monitored by the Headteacher, DSL, and the governors.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

3.0 Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'

4.0 Roles and responsibilities

4.1 The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL and DDSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place across both schools
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with hardware support and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

4.2 The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL, DDSL and SLT to conduct light-touch reviews of this policy.

4.3 The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO, Computer lead and Hardware support.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

4.4 All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data, they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

4.5 Pupils will be responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

5.0 Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Headteacher has overall responsibility for the school's approach to online safety, with support from DSL's, the Computer lead and Hardware support. The Headteacher / DSL / DDSL's should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Our Internet access provides a service designed for pupils, including a "firewall" filtering and monitoring system through SWGFL; intended to prevent access to material inappropriate for children.

- Children using the Internet will usually be working in the classroom on laptops or iPads and will always be supervised by an adult.
- Staff will aim to check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- If staff or pupils discover an unsuitable site, it will be reported to the Class Teacher and then Computing Leader or Hardware who will ensure that it is subsequently blocked.
- Staff will be particularly vigilant when pupils are undertaking their own research and will check that the children are following the agreed home/school agreement.
- Pupils will have access to information from relevant outside agencies.
- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Workshops, Computing lessons and PSHE lessons are conducted on the topic of remaining safe online

6.0 Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the Chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Inclusion team and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

7.0 Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.
- The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

- Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying and Hate Policy.

8.0 Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

For further information refer to the school's Safeguarding Policy.

9.0 Online safety training for staff

The Headteacher / DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

10.0 Online safety and the curriculum

Online Safety incorporates Internet Technology and electronic communications such as mobile phones and other wireless technology. Technology is constantly changing at home and in the community; its impact on the lives of individuals continues to grow, therefore, it is essential to educate children about the benefits and risks of using new technology.

At Ruardean C of E Primary School, online safety is embedded throughout the curriculum and pupils will be taught about online safety as part of the National curriculum for computing. It will also be addressed in the following subjects:

- PHSE
- Relationships and Health Education
- Online Safety / Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- Using technology safely and respectfully, keeping personal information private
- Recognise acceptable and unacceptable online behaviour
- Identify where to go for help if they have concerns about online content or contact
- Identify a range of ways to support concerns about online content and contact

The DSL / DDSL's will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and pupils considered vulnerable.

Class teachers will aim to review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding Policy.

11.0 Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will aim to review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

11.1 Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Home School Agreement for Pupils.

Pupils are not permitted to have mobile phones upon their person at any point within the school day. Some pupils may have permission from the Headteacher to have their mobile phones on school premises however these are to be handed into the school office and locked away until the end of the school day.

Smart Watches will not be allowed in school if they have the ability to record or take photos. The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

11.2 AI

The school has a separate policy for the use of AI in school.

12.0 Educating parents and carers

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be signposted to this policy and the Home School Agreement.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Information through ParentPay communication
- School websites
- Information on Friends of Ruardean Facebook group
- Online resources

13.0 Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

Deliberate breaches of the filtering system will be reported to the DSL and hardware support, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

14.0 Emails

Staff, governors and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Children's personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

When sending emails internally children's initials will be used rather than names.

The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

15.0 The school website

The Headteacher, Staff and Administrators are all responsible for the content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website will be checked at least annually by Governors and external reviews will be commissioned.

16.0 Monitoring and review

The governing board, Headteacher and DSL will review this policy every two years.

Any changes made to this policy are communicated to all members of the school community.

17.0 Links to other policies:

Safeguarding Policy

Health and Safety Policy

Behaviour Policy

SEND and inclusion policy

Anti Bullying Behaviour Policy

AI Policy

Staff code of conduct

Whistleblowing

Allegations against staff

Appendix 1 Pupil/Parent Agreement

Ruardean Church of England Primary School Pupil Acceptable Use Agreement / E-safety Rules

Dear Parent/ Carer,

ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these E-safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact your child's class teacher.

Pupil Acceptable Use Agreement / E-safety Rules:

- I will only use ICT in school for schoolwork or homework.
- I will not use my own personal email in school.
- I will not bring a mobile phone or smart watch to school.
- I will only login using my class name.
- I will only open or delete my own files.
- I will only print once permission has been granted.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I accidentally find anything like this, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my E-safety.

We have discussed acceptable use and(child name) agrees to follow the E-safety rules and to support the safe use of ICT at Ruardean C of E Primary School.

Parent/ Carer Signature

Class Date

Appendix 2 Staff/Visitors Agreement –

Acceptable Use Agreement / Code of Conduct

Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that staff, governors or visitors are aware of their professional responsibilities when using any form of ICT in school. Staff, governors or visitors are expected to sign this policy and at all times adhere to its contents. Any concerns or clarification should be discussed with the school E-safety coordinator.

- I will only use the school's computers for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will not use my mobile phone or smart watch for personal use in the presence of pupils.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware or software onto school computers without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies in school can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

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

SignatureDate
Full Name(printed)
Job title

MS Form Version Sent Annually in January and to new starters on joining:
<https://forms.office.com/e/9D8JJdULwD>