# Rathmore Primary School



# Acceptable Use of the Internet and Online Safety Policy

| Date Ratified: | May 2025 |
|---|---|
| Date of Review: | In line with the school's schedule for policy review. |

This policy has been written following a consultation process, ratified by the Board of Governors and communicated to the school community as required. It will be monitored and reviewed as part of the school's policy review schedule.

## Article 13

**Every child must be free to express their thoughts and opinions and to access all kinds of information, as long as it is within the law.**

The Board of Governors will ensure that Rathmore Primary School has a policy on the safe, healthy, acceptable and effective use of the Internet and other digital tools e.g. digital cameras, acceptable use of mobile phones and gaming hand-held equipment which has downloadable capabilities e.g. smart phones, watches or PSP's. They also promote safe and acceptable practices for all staff and children.

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the Internet technologies children are using, both inside and outside of the classroom, include:

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

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

In Rathmore Primary School we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the classroom.

The Internet

The Internet is a unique and exciting resource.  It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that

using the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable.

Key Concerns are:

- Potential Contact: Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons.

Children should be taught:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details.
- That they should never meet alone anyone contacted via the Internet.
- That once they publish information it can be disseminated with ease and cannot be reclaimed.

Inappropriate Content

On the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children. Materials may express extreme views or may contain misleading and inaccurate information.

Children should be taught:

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests.

Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety.
Teachers, pupils and parents must be vigilant.

Risk assessments:

There are a number of risks linked to using modern technologies and accessing the Internet. Pupils are advised and made aware of the necessary actions to take if they come across anything inappropriate. Staff are vigilant to look out for anything inappropriate and risk assessments have been put in place to ensure that any risk is minimised.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Leader to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

The Principal/ICT Leader update School Leaders and Governors with regard to e-safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

E-Safety Skills Development for Staff

All staff receive information and training on e-safety issues.

• All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
• New staff members receive information on the school's Acceptable Use Agreement as part of their induction.
• All staff are encouraged to incorporate e-safety activities and awareness within their lessons.

E-Safety Information for Parents/Carers

• Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
• Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used by the school.
• The school will communicate relevant e-safety information through newsletters and the school website/seesaw app.

Advice to Parents

Parents should remember that it is vital to promote e-safety in the home and to monitor Internet use.

- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Consider using parental controls and safe search filters.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people online may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet online.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning Internet

- The school will plan and provide opportunities within a range of curriculum areas to teach e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school C2k Internet access is filtered through the C2k managed service.
- Google set to safe search automatically.
- No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.

Social Networking:

- The school C2k system will block access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school. School staff will not add children as 'friends' if they use these sites.

Mobile Technologies:

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks or mobile phones.
- Pupils are not allowed to use personal mobile devices/phones during school hours.
- Staff should not use personal mobile phones during designated teaching sessions except with the consent of the principal. An exception is when a member of staff is in a particular part of the school and is following technical instructions from an engineer. Teachers and classroom assistants may use mobile phones (if required) when taking children out of school, for example, when travelling to and from the swimming pool,

on a single day trip or residential visits. Any individual can be contacted via the school telephone if there is an emergency.

Publishing Pupils' Images and Work:

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or on Seesaw. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances and school is notified, in writing, by the parent/carer.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

The use of AI

We will keep parents informed about the school's use of AI via Seesaw and website updates. Should parents have any concerns about the use of emerging technologies in school, they are encouraged to contact the school office.  School will seek consent from parents/carers before a pupil's intellectual property is entered into an AI tool.

Should staff wish to make use of AI, this request will be considered by School Leaders in line with school safety practices and data protection measures.

Through ICT and PDMU lessons, pupils will be taught about the responsible and ethical use of AI as a support tool.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-safety rules. These e-safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-safety rules and within the constraints detailed in the school's e-safety policy.
- All staff must read and agree to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, SIM systems.

Handling E-Safety Complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Leader and/or recorded by the school's Designated Teacher/Safeguarding Team.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

Communicating the Policy:

Introducing the e-safety Policy to pupils

- E-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils each year. Lessons will be taught by class teachers every year linked to curriculum areas such as PDMU.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the E-Safety Policy:

All staff will be given the School e-Safety Policy and its importance explained.

- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop or tablet issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.
- Devices issued to parents for Home Learning remain the property of the school. Parents must sign for the device and agree to follow school procedures.

Writing and Reviewing the E-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Child Protection, and Antibullying.

It has been agreed by the Senior Leaders, Staff and approved by the Governing Body. The e-safety policy and its implementation will be reviewed annually.