Bridgewater Primary School
Bridgewater Street
Little Hulton
Salford
M38 9WD

Online Safety Policy

Reviewed November 2023

To be reviewed September 2024

Rationale

The Internet is an essential element in 21st century life for education, business and social interaction. We have a duty to provide our learners with Internet access as part of their learning experience. Bridgewater Primary School believes that this access must ensure the safeguarding of all learners.

Subject Coordinator:	Website Coordinator:	Child Protection Officer:
Tom Tien-Rhimes	Tom Tien-Rhimes	Emma Henderson

Internet Use to Enhance and Extend Learning

- Bridgewater's Internet access is designed expressly for pupil use and includes RM filtering and monitoring appropriate to the age of pupils.
- Clear boundaries will be set for the appropriate use of the internet and digital communications and discussed with staff, pupils and parents.
- Pupils will be educated in the effective use of the Internet in research, how to critically evaluate the materials they read and shown how to validate information before accepting its accuracy through our Computing curriculum.
- We will ensure that the use of Internet derived materials will comply with copyright law.

Managing Internet Access

Information system security

- Bridgewater's system security will be reviewed regularly by blocking any inappropriate content by informing RM. If something that is blocked which shouldn't be, a request to unblock it will be sent.
- Virus protection will be installed and updated regularly by the RM Managed Service.
- Live monitoring of internet usage on all school devices is powered by SmoothWall Monitor and provides the school safeguarding team with real time updates relating to any safeguarding concerns or inappropriate internet use.

E mail and Messaging

- Pupils must immediately tell a teacher if they receive an offensive email or message.
- In any email communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Attachments should be treated as suspicious and not opened unless the author is known.
- The forwarding of chain emails is not allowed.

Published content on the school website

- Any online contact details for staff should be their salford.gov.uk email address or the school office. Any pupil contact details must be the school office.
- Staff are to keep up to date lists of children who cannot be photographed and ensure that work in books or for the website comply.
- The member of staff given overall responsibility for the website will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include students will be carefully selected so that individual pupils cannot be identified or their image misused.
- Students' full names will not be used anywhere on the school website, particularly in association with photographs.

- Written permission from parents will be obtained before photographs of students are published on the school website.
- Work can only be published with the permission of the pupil.

Social Networking and personal publishing

- Bridgewater will control access to social networking sites, and consider how to educate pupils in their safe use.
- School issues should not be discussed on social networking sites by staff or parents of children.
- Newsgroups will be blocked unless a specific use is approved by the subject coordinator.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils are encouraged to set strong passwords, to deny access to unknown individuals and block unwanted communication. Only known friends should be invited and access denied to others.

Managing Filtering and Monitoring

- The school will work in partnership with the RM Managed Service to ensure that the systems in place to protect our pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Co-ordinator and RM to be blocked.
- Regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- SmoothWall Monitor provides real time monitoring of internet use on all school devices and provides updates to the safeguarding team where a safeguarding/ inappropriate content concern is raised.

Managing Videoconferencing

- IP videoconferencing rights and privileges will be monitored and controlled by the coordinator.
- Pupils must seek permission from the supervising teacher before answering or making a videoconference call.
- Videoconferencing must appropriately be supervised for the pupils' ages.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed.
- Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Therefore, mobile phones should not be used at any time during the school day by pupils, and only in designated zones by staff.
- Staff should not contact students directly with their own mobile phones unless in exceptional circumstances and a member of the SLT has been informed.
- Staff should be vigilant to avoid the receipt of items via Bluetooth, Airdrop whilst in school.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff are not permitted to use personal USB/ Storage devices in school. If staff require a storage device for work purposes then are able to request an encrypted devices from the computing lead, Tom Tien-Rhimes.

- Staff are encouraged to use safe passwords which contain lower case, upper case and special characters and numbers.

Acceptable Use
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users should not engage in these activities in school or outside school when using school equipment or systems. Any reports of such materials or activities should be passed onto the coordinator and if necessary the Child protection officer. The school policy restricts certain internet usage as follows:

- ✓ Reference to terrorism and extremist materials,
- ✓ pornography,
- ✓ promotion of any kind of discrimination based on protected characteristics
- ✓ promotion of racial or religious hatred
- ✓ child sexual abuse images
- ✓ promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- ✓ adult material that potentially breaches the Obscene Publications Act in the UK
- ✓ threatening behaviour, including promotion of physical violence or mental harm
- ✓ any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- ✓ Using school systems to run a private business
- ✓ Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school
- ✓ Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- ✓ Creating or propagating computer viruses or other harmful files
- ✓ On-line gambling
- ✓ Accessing the internet for personal or social use (e.g. online shopping, banking etc)
- ✓ File sharing e.g. music, films etc
- ✓ Use of social networking sites

<u>Policy Decisions</u>

Sharing the Online Safety & Mobile Technology Policy
- All staff must read and sign the 'Staff Code of Conduct for ICT' to allow use of the school resources.
- A list of all current staff and pupils granted access to school ICT systems will be maintained.
- Pupils must also apply for Internet access individually by agreeing to comply with the Responsible Use Statement on view in all rooms with ICT resources.
- Parents/Carers are also asked to sign and return a consent form.

Assessing Risks
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school, nor Salford LA can accept liability for any material accessed, or any consequences of Internet access.
- The school will annually audit ICT use to establish if the Online Safety & Mobile Technology policy is adequate and that the implementation of the policy is appropriate and effective.

Handling Complaints

- Complaints of Internet misuse will be dealt with by the Online Safety Coordinator.
- Any complaints about staff misuse must be referred to the Online Safety Coordinator and the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures.
- Discussions will be held with the Police or Community Support Officers to establish procedures for handling potentially illegal issues.

Communicating Online Safety

Sharing the Online Safety & Mobile Technology policy with Pupils

- Online Safety rules will be posted in all rooms where computers are used.
- Pupils will be informed that network and internet use will be monitored.
- Training in Online Safety will be developed based on the materials provided by the Child Exploitation and Online Protection centre (CEOP) and delivered to pupils via assemblies and through lessons in class relevant to their age.

Staff and the Online Safety & Mobile Technology policy

- All staff will be given the policy and its importance will be explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff managing filtering and monitoring systems and monitoring ICT use will be overseen by the Coordinator and work to clear procedures for reporting issues (see appendix).

Enlisting Parents' and Carers' Support

- Parents' and carer's attention will be drawn to the school Online Safety & Mobile Technology policy in the prospectus, on the school website, via parent evenings and an annual Online Safety Workshop will be held.
- Parent workshops run by the Computing Subject Lead will inform parents about how online safety is taught and why it is important.

Appendix 1

Online Safety & Mobile Technology policy Summary for Parents

What is Online Safety?

Online Safety encompasses the use of new technologies, Internet and electronic communications such as mobile phones, Ipads and electronic tablets, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible I.C.T. and Computing use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of Online Safety & Mobile Technology policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Salford including the effective management of filtering and monitoring.

Writing and reviewing the Online Safety & Mobile Technology policy

- The Online Safety & Mobile Technology policy relates to other policies including those for Computing, Anti-Bullying and for Child Protection.
- Our Online Safety & Mobile Technology policy has been written by the school and from government guidance. It has been agreed by senior management and approved by the Governors.
- The Online Safety & Mobile Technology policy and its implementation will be reviewed annually.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering and monitoring appropriate to the age of pupils.
- 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. Pupils will be taught how to evaluate Internet content.
- 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.

Managing Internet Access

Information system security

- School I.C.T. systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Salford.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive 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.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school web site. This is done on entry to school.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- School issues should never be discussed on social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

- The school will work with the LA, DFES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
- The Coordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are not permitted at any time in school. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff are not permitted to use personal USB/ Storage devices in school. If staff require a storage device for work purposes then are able to request an encrypted devices from the computing lead, Tom Tien-Rhimes.
-

Policy Decisions

Authorising Internet Access

- All staff pupils and parents must read and adhere to the 'Acceptable I.C.T. Use Agreement' before using any school I.C.T. resource.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Salford City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit I.C.T. provision to establish if the Online Safety & Mobile Technology policy is adequate and that its implementation is effective.

Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by the Online Safety Coordinator.
- Any complaint about staff misuse must be referred to the Online Safety Coordinator and the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- External organisations using the school's I.C.T. facilities must adhere to the Online Safety & Mobile Technology policy.

Communicating the Online Safety & Mobile Technology Policy to Children

Introducing the Online Safety & Mobile Technology policy to pupils

- Children will sign the Online Safety agreement before being allowed to use the network and internet.
- Online Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year and on regularly occasions throughout their computing curriculum and use of mobile technologies in other subjects.
- Pupils will be informed that network and Internet use will be monitored.

Tom Tien-Rhimes
Deputy Headteacher/ Computing Lead

Appendix 2

Staff Code of Conduct for ICT, Online Safety & Mobile Technology

BRIDGEWATER
PRIMARY SCHOOL

To ensure that all members of staff are fully aware of their professional responsibilities when using information systems and when communication with pupils, you are asked to sign this code of conduct. Members of staff should consult the school's **Online Safety & Mobile Technology Policy** for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, Ipads and electronic tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Coordinator or Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I am aware that images and text posted on public sites may be viewed by pupils and their parents. I will strive to ensure that my professional status will not be affected by anything I post in the public domain.
- I will not discuss school issues on any social networking sites.
- I will ensure that electronic communications on social networking sites (e.g. facebook) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that electronic communications with pupils including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software of hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any instances of concern regarding children's safety to the Online Safety Coordinator and the Designated Child Protection Coordinator.
- I will promote Online Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I understand that breeches of this Code of Conduct may result in disciplinary action being taken.

Acceptable Use

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems.

- ✓ Reference to terrorism and extremist materials,
- ✓ pornography,
- ✓ promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability
- ✓ promotion of racial or religious hatred
- ✓ child sexual abuse images
- ✓ promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- ✓ adult material that potentially breaches the Obscene Publications Act in the UK
- ✓ threatening behaviour, including promotion of physical violence or mental harm
- ✓ any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- ✓ Using school systems to run a private business
- ✓ Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school
- ✓ Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- ✓ Creating or propagating computer viruses or other harmful files
- ✓ On-line gambling
- ✓ Accessing the internet for personal or social use (e.g. online shopping, banking etc)
- ✓ File sharing e.g. music, films etc
- ✓ Use of social networking sites

Bridgewater Primary School may exercise its right to monitor the use of the school's information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT, online Safety & Mobile Technology:

Signed: **Name:** **Date:**

Appendix 3

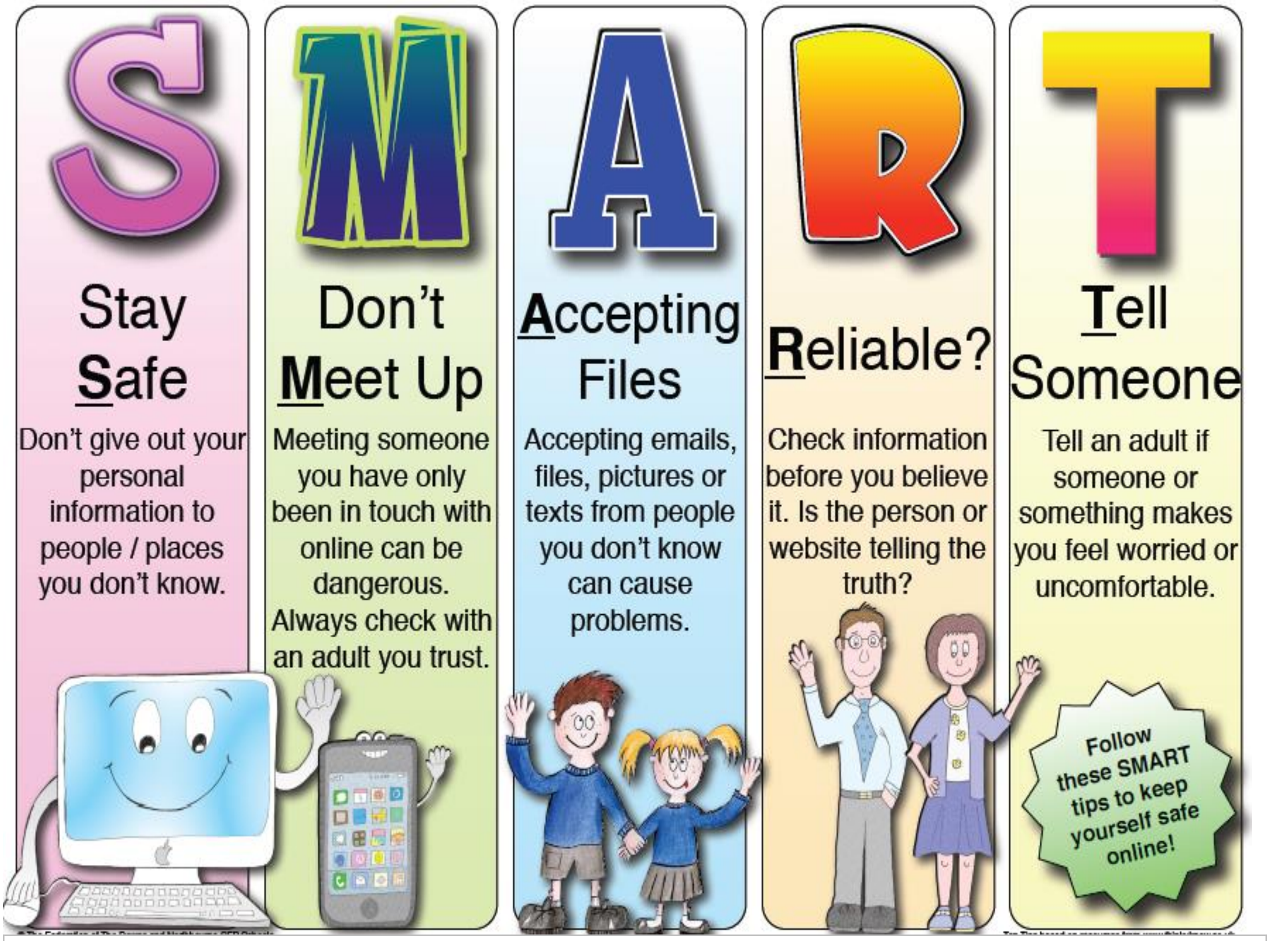
Bridgewater Primary School

Online Safety Rules

These Online Safety & Mobile Technology Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information including passwords through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the ICT Coordinator or head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- The school ICT systems must not be used for any message or activity which could be considered to be cyberbullying.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.



Stay **S**afe

Don't give out your personal information to people / places you don't know.

Don't **M**eet Up

Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.

Accepting Files

Accepting emails, files, pictures or texts from people you don't know can cause problems.

Reliable?

Check information before you believe it. Is the person or website telling the truth?

Tell Someone

Tell an adult if someone or something makes you feel worried or uncomfortable.

BRIDGEWATER
PRIMARY SCHOOL

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety & Mobile Technology Rules have been understood and agreed.

Pupil:	***Class:***

Pupil's Agreement

- I have read and I understand the school Online Safety& Mobile Technology Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I will not use the network and Internet for anything which may be considered online bullying.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Appendix 5

Bridgewater Primary School

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety & Mobile Technology Rules have been understood and agreed.

Pupil:	***Class:***

Parent's Consent for Web Publication of Work and Photographs **(please tick)**

I agree that my son/daughter's work may be electronically published. □

I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names. □

Parent's Consent for Internet Access

I have read and understood the school Online Safety & Mobile Technology rules and give permission for my son / daughter to access the Internet.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

Signed: ***Name:***	***Date:***