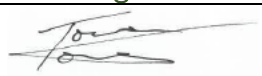
SHERSTON C OF E

PRIMARY SCHOOL

# Online Safety Policy

| Date Approved | Review Date | Signed |
|---|---|---|
| Sept 2025 | Sept 2026 |  |

| Year | Amendments (in Yellow) |
|---|---|
| 2023 | Implement vision<br>Policy name change<br>Location of Online Safety Rules |
| 2024 | Added Oakford to groups involved in online safety<br>Point added regarding Y5 & 6 mobile phones for walking home alone |
| 2025 | Added sections around AI & misinformation, disinformation, fake news and conspiracy theories as per KCSiE 25 |

## Statement of intent

At Sherston CE Primary School, we are dedicated to providing a safe and nurturing environment where all members of our school community can embrace the opportunities of the digital age. Our vision 'Learning, Caring and Achieving Together' guides our commitment to equipping our students with the knowledge, skills, and values necessary to navigate the online world responsibly and confidently.

In an era where technology plays a fundamental role in education and communication, we recognise the importance of fostering a culture of online safety. Our intent is clear: we aim to create a digital ecosystem where children, staff, parents, and guardians learn, connect, and collaborate in a secure and respectful manner. We believe that by working together as a community, caring for each other's digital well-being, and achieving a high standard of online conduct, we can ensure that the internet becomes a valuable tool for learning and communication, rather than a source of harm or disruption.

This Online Safety Policy is a testament to our commitment to the well-being of our children and the promotion of responsible digital citizenship. It outlines our strategies and expectations for maintaining a safe online environment within our school and provides a framework for continuous education and improvement. Together, we can harness the power of technology to enhance our educational journey while safeguarding the welfare of our children.

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4/5G connections now mean the world wide web is available anywhere, anytime. Moreover, the introduction of the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our children from the dangers hidden in cyberspace.

Our children will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

As a result, designing and implementing an Online Safety Policy demands the involvement of a wide range of interest groups: the governors, headteacher, SLT, SENDCO, DSL, classroom teachers, support staff, school ICT technicians (Oakford), young people or parents, LA personnel, internet service providers (ISP), and regional broadband consortia, working closely with ISPs on network security measures.

Online Safety is a child protection issue, and indeed it should not be managed primarily by the Computing Leader. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

Together, we can harness the power of technology to enhance our educational journey while safeguarding the welfare of our children. We will ensure children are equipped to safely and responsibly engage with emerging technologies, such as artificial intelligence (AI), and are educated on recognising and responding to misinformation, disinformation, fake news, and conspiracy theories to develop critical thinking and resilience online.

An Online Safety Policy should:

- Allow young people to develop their own protection strategies for when adult supervision and technological protection are not available.
- Give information on where to seek help and how to report incidents.
- Help young people understand that they are not accountable for the actions that others may force upon them but that there are sanctions that the school will impose if they act inappropriately when online.
- Provide guidelines for parents and others on safe practice.
- Ensure you regularly monitor and review your policies with stakeholders.
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective Online Safety programme.

Above all, Online Safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.

## 1. Teaching and learning

### Why the internet and digital communications are important

1.1. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

1.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

1.4. Staff model safe and responsible behaviour in their use of technology during lessons.

### Internet use will enhance learning

1.5. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

1.6. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

1.7. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
1.8. Pupils will be shown how to publish and present information to a wider audience.

### Pupils will be taught how to evaluate internet content

1.9. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
1.10. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
1.11. Pupils will be taught how to report unpleasant internet content to a trusted adult. This can be done anonymously, or in person, and will be treated in confidence.
1.12. Pupils will learn how to identify misinformation, disinformation, fake news, and conspiracy theories and understand the potential impact these can have on individuals and society.
1.13. Pupils will be encouraged to question the origin and reliability of online content, including content generated by AI systems.
1.14. The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience. We follow the SWGFL Digital citizens' scheme.

## 2. Managing internet access

### Information system security

2.1. School ICT systems security will be reviewed regularly.
2.2. Virus protection will be updated regularly.
2.3. Security strategies will be discussed with the LA at least annually.

### Email

Pupils do not have access to email on the school system.

2.4. The school:

- Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal email should be through a separate account.
- Does not publish personal email addresses of pupils or staff on the school website.
- Will contact the police if one of our staff or pupils receives an email that it considers is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

### Published content and the school website

2.5. Staff or pupil personal contact information will not be published.
2.6. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.
2.7. Uploading of information is restricted to our website authorisers. This includes class teachers and administrators.

2.8. The school website complies with the following statutory DfE guidelines for publications: What maintained schools must publish online

2.9. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

2.10. The point of contact on the website is the school address and telephone number. The school uses a general email contact address, e.g. admin@sherston.wilts.sch.uk. Home information or individual email identities will not be published.

2.11. Photographs of pupils published on the web do not have full names attached.

2.12. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

## Publishing pupils' images and work

2.13. Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. The school will consider using group photographs rather than full-face photos of individual children.

2.14. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

2.15. Written permission from parents will be obtained before photographs of pupils are published on the school website.

2.16. Work can only be published with the permission of the pupil and parents.

2.17. Pupil image file names will not refer to the pupil by name.

2.18. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.19. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

2.20. The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

2.21. Staff sign the school's Staff Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.

2.22. If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, the school will obtain individual parental or pupil permission for their long-term use.

2.23. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

2.24. Pupils are taught about how images can be manipulated in their Online Safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

2.25. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

2.26. Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

## Managing filtering

2.27. If staff or pupils come across unsuitable online materials, the site must be reported to the Headteacher.

2.28. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

## Managing emerging technologies

2.29. Emerging technologies, including artificial intelligence tools, will be examined for educational benefit and a thorough risk assessment will be carried out before use in school is allowed. Guidance will be provided for staff and pupils on the safe, responsible, and ethical use of AI technologies, including awareness of data privacy, bias, and potential misuse. AI will not be used to replace professional judgement in safeguarding or educational decisions.

2.30. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

2.31. Mobile phones will not be used during school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

2.32. Pupils are not permitted mobile phones on site. Phones for walking home alone are stored in the school office during the day and given to the child at home time, as they leave the building.

2.33. Staff will not use personal mobile phones to communicate with children or use them to capture images of them.

## Protecting personal data

2.34. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

## Personal devices and mobile phones

2.35. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Headteacher.

2.36. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

2.37. Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the office staff to answer on their behalf or seek specific permissions to use their phone at other than their break times.

2.38. Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times.

2.39. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

2.40. No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

2.41. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

2.42. Staff will be issued with a school phone where contact with pupils' parents is required.

2.43. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

2.44. Pupils will abide by the following rules when using personal devices in school:

- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. (see separate guidance on website)
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place, and devices will be released to parents.
- If a pupil needs to contact their parents, they will be allowed to use a school phone.
- No pupil should bring their mobile phone or personally-owned device into school without a signed consent form from their parents/carers.
- Pupils in year 5 & 6 require permission from parents to bring in mobile phones and leave them at the school office to keep until the end of the day so that they have it when walking home alone.

## Policy Decisions

### Authorising internet access

2.45. All staff will read and sign the Code of Conduct before using any school ICT resource.

2.46. At EYFS and in KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

### Assessing risks

2.47. 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 the LA can accept liability for any material accessed, or any consequences of internet access.

2.48. The school should audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

### Handling Online Safety complaints

2.49. Complaints of internet misuse will be dealt with by a senior member of staff.

2.50. Any complaint about staff misuse must be referred to the Headteacher.

2.51. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see appendix).

2.52. Pupils and parents will be informed of the complaints procedure (see school's complaints policy)

2.53. Pupils and parents will be informed of the consequences for pupils misusing the internet.

2.54. Discussions will be held with the police or MASH to establish procedures for handling potentially illegal issues.

## 3. Pupil online safety curriculum

### Teaching and learning

3.1. This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children. We use the SWGFL Digital citizens' programme.

3.2. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

3.3. The school will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement which every pupil will sign.

3.4. All staff will model safe and responsible behaviour in their own use of technology during lessons.

### Online risks

3.5. The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE/Digital Citizenship) that some adults and young people will use such outlets to harm children. The curriculum will also include teaching about the risks associated with AI-generated content, deepfakes, and misleading or false information online. Children will learn strategies to verify information, think critically about sources, and avoid spreading unverified content. This includes recognising misinformation, disinformation, fake news, and conspiracy theories.

### Cyber bullying and abuse

3.6. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." - BullyingUK

3.7. Complaints of online bullying are dealt with in accordance with our Behaviour Policy. Complaints related to child protection are dealt with in accordance with school/LA safeguarding/child protection procedures.

3.8. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

3.9. Posters providing information about how to get help from NSPCC Childline and CEOP are displayed in classrooms and along the corridors of the school.

3.10. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated.

### Sexual exploitation/sexting

3.11. All incidents of sexting reported to the school will be recorded and dealt with through child protection procedures.

### Radicalisation or extremism

3.12. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

3.13. Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:
- Encourage, justify or glorify terrorist violence in furtherance of beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.
- Foster hatred which might lead to inter-community violence in the UK."

3.14. The school understands that here is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

3.15. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.

3.16. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

3.17. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

3.18. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

## 4. Communications policy

### Introducing the Online Safety Policy to pupils

4.1. Online Safety rules will be in PSHE books and discussed with pupils regularly.

4.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

4.3. Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

### Staff and the Online Safety policy

4.4. All staff will be given the school Online Safety Policy and have its importance explained.

4.5. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

4.6. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

4.7. Staff will always use a child friendly safe search engine when accessing the web with pupils.

### Enlisting parents' support

- The school will provide parents with Online Safety information via the twice termly newsletter.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.

- The school will provide parents with useful links to help them in understanding the internet.

| Activities | Key Online Safety issues |
|---|---|
| Creating web directories to provide easy access to suitable websites | • Parental consent should be sought<br>• Pupils should be supervised<br>• Pupils should be directed to specific, approved online materials |
| Using search engines to access information from a range of websites | • Filtering must be active and checked frequently<br>• Parental consent should be sought<br>• Pupils should be supervised<br>• Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with |
| Exchanging information with other pupils and asking questions of experts via email or blogs | • Pupils should only use approved email accounts or blogs<br>• Pupils should never give out personal information |
| Publishing pupils' work on school and other websites | • Pupil and parental consent should be sought prior to publication<br>• Pupils' full names and other personal information should be omitted<br>• Pupils' work should only be published on moderated sites and only by the school administrator or class teacher |
| Publishing images, including photographs of pupils | • Parental consent for publication of photographs should be sought<br>• Photographs should not enable individual pupils to be identified<br>• File names should not refer to the pupil by name<br>• Staff must ensure that published images do not breach copyright laws |
| Communicating ideas within chat rooms or online forums | • Only chat rooms dedicated to educational use and that are moderated should be used<br>• Access to other social networking sites should be blocked<br>• Pupils should never give out personal information |
| Audio and video conferencing to gather information and share pupils' work | • Pupils should be supervised<br>• The school should only use applications that are managed by LAs and approved educational suppliers |
| Social networking | • Staff should set their profiles to private and ensure they do not accept friend requests from pupils or parents<br>• Social networking sites should be blocked on the school network<br>• Pupils should be educated in the dangers involved in 'friending' or talking to people they do not know online |

| Resource | Website |
|---|---|
| Child Exploitation and Online Protection Centre | www.ceop.gov.uk/ |
| Childnet | www.childnet-int.org/ |
| Kidsmart | www.kidsmart.org.uk/ - Now part of Childnet |
| Think U Know | www.thinkuknow.co.uk/ |
| Family Online Safety Institute | http://www.fosi.org |
| Internet Watch Foundation | www.iwf.org.uk |
| Vodafone digital parenting | www.vodafone.com/content/digital-parenting.html |
| NSPCC | https://www.nspcc.org.uk/keeping-children-safe/onlinOnline Safety/ |
| Parent Zone | https://parentzone.org.uk/ |

## Response to an Incident of Concern Flowchart

The process outlined within the first section should be followed where a staff member has a safeguarding concern about a child. Where a referral has been made, the process outlined in the 'After a referral is made' section should be followed.

The actions taken by the school are outlined in yellow, whereas actions taken by another agency are outlined in blue.

Before a referral is made

A staff member identifies a concern or potential concern. Is the pupil at immediate risk of harm?

N

Is the DSL or the deputy DSL available to discuss the concern with?

Y

The staff member immediately notifies the police of the situation and informs the DSL.

Y

The staff member discusses the concern with the DSL. Taking into account observations and using professional judgement, is a referral required?

N

The staff member makes a referral to children's social care services (CSCS), notifying the DSL of this as soon as possible.

Y

The DSL makes a referral to CSCS, keeping the staff member who raised the concern up-to-date with what action is taken.

N

The pupil continues to be monitored and early help is provided where necessary. If the concern escalates, a referral is made to the CSCS.

Within one working day, a social worker from CSCS will make a decision about the type of response that is required and will notify the referrer. Where this information is not forthcoming, the referrer should contact the appointed social worker to follow up the referral.

The steps outlined in the next flowchart are then followed.

## After a referral is made

Once a referral has been made, a social worker from CSCS will notify the referrer that a decision has been made and one of the following responses will be actioned.

The pupil is in need of immediate protection.

Where the pupil is at risk of significant harm but is not in immediate danger, a strategy discussion is held.

No formal assessment is needed.

Where appropriate to do so, the DSL and staff member who raised the concern may be consulted during these stages to ensure that all areas of concern are addressed.

The DSL supports the initial staff member to liaise with other agencies to arrange an early help assessment and appropriate support.

Appropriate emergency action is taken by the social worker, police or NSPCC.

A Child in Need assessment is completed within 45 working days.

Within 15 working days of the strategy discussion, an initial child protection conference is held.

A child protection plan is potentially required.

The type of support needed is identified, arranged through multi-agency liaison and provided effectively.

Staff keep the pupil's circumstances under review and re-refer if appropriate to ensure circumstances improve – the pupil's best interests always come first.

If the child's situation does not appear to be improving, the DSL should press for re-consideration to ensure their concerns have been addressed and, most importantly, that the child's situation improves.

aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the headteacher.

- I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing board.
- 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 personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the headteacher or governing board and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the headteacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- 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 data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or headteacher in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the 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. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).

- I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

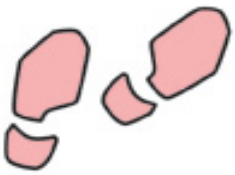
Rules for EYFS and KS1

# Think then Click

These rules help us to stay safe on the internet

Online Safety rules for EYFS and KS1

- ✓ We only use the internet when an adult is with us.
- ✓ We can click on the buttons or links when we know what they do or where they take us.
- ✓ We can use the internet to search for things when an adult is with us.
- ✓ We always stop and ask for help if we get lost on the internet.
- ✓ We can send and open emails with a grown-up.
- ✓ We can write polite and friendly emails to people we know.
- ✓ We never share our names or addresses on the internet.
- ✓ We know that friends are people we know in the real world not people we meet online.




Rules for KS2

# Think then Click

These rules help us to stay safe on the internet

Online Safety rules for KS2

- ✓ We ask permission before using the internet.
- ✓ We only look at websites an adult has given us permission to use.
- ✓ We always tell an adult if we have seen, heard or read anything on the internet that has made us feel threatened, uncomfortable or worried.
- ✓ We immediately close a web page if we are unsure.
- ✓ We only send polite and friendly emails to people we know or that an adult has approved.
- ✓ We never give out personal information or passwords.
- ✓ We never arrange to meet anyone we don't know.
- ✓ We do not open emails sent by anyone we don't know.
- ✓ We do not use internet chat rooms.
- ✓ We know that friends are people we know in the real world not people we meet online.