Abingdon Primary School
Acceptable Use Policy including E-safety rules

These rules aim to help to **protect children, young people and adults** by describing acceptable and unacceptable use of digital equipment.

- It is a **criminal offence** to use a computer or network or any other digital equipment **for a purpose not permitted by law**. Illegal activities include downloading copyrighted music, films and harassing other people on-line. Distributing sexual pictures of young people is illegal.

- If anyone is found to be involved in criminal activity then the police will be informed and be given our full cooperation in any subsequent investigation. If anyone is found to be behaving irresponsibly then appropriate disciplinary measures may be invoked.

- Irresponsible use may result in the confiscation of equipment or the loss of network/ Internet access.

- Network access must only be made via the user's authorised account and password.

- **Passwords must not be shared**. If you think someone else knows your password then you should change it as soon as possible. Passwords should be a combination of upper and lower case letters, numbers and other characters. They should not be written down and kept with the equipment.

- When you are on-line or on the phone you should behave in the same way that you would if you were talking to that person face-to-face. Messages should be written carefully and politely. Information posted on websites too. Consider what other people may do with the information once it is in the public domain.

- All communication should reflect and promote the positive ethos of the school. Consider wording carefully when using digital communication and note that any named groups or wording involving the school is considered under this umbrella.

- Users should take care **never to reveal personal information** without permission, either about themselves or other people, via digital technology. **This may include passing on email or mobile phone contact details, uploading or downloading images.** If you are not sure, ask the person whose information you are passing on whether they are happy for their details to be shared. Remember, once the information is out there it is beyond your control. Future employers, friends and the rest of your family may all have access.

- Copyright and intellectual property rights must be respected. Please consider when you are uploading or downloading items whether you are authorised to do this. This includes plagiarism as well as music and films.

- Promote good network practice. Make sure that you have closed down applications properly when you have finished your session. Make sure that you have stored information appropriately especially if it is personal and confidential.

- Wherever possible do not use your personal equipment for work purposes. Ask if you can be provided with a mobile phone for trips. If you are expected to provide photographs consider using a disposable camera rather than your personal digital version. Using your own equipment may make you vulnerable to accusations of misuse or open to unwanted personal harassment.

- be a SMART user:

  - Keep SAFE by being careful not to give out personal information to anyone you don't know. Otherwise you don't know where it will end up, what it will be used for or who may contact you.
  Remember that once you send something to another phone or the internet it can easily be copied or changed or stay on-line forever.
  If you have your own web-space make sure it's set up so that only the people you want to access it can!

  - Never feel pressurised to MEET on-line friends. In reality, some people may not be who they pretend to be on-line. It's difficult to remember that people you've been chatting to for a while on-line are really strangers and not good friends. If you want to meet up then arrange it during the day, in a public place and take someone with you.

  - If you ACCEPT files or emails from people you don't know then you may be putting your computer at risk of viruses or yourself at risk of junk mail or unsuitable/ nasty messages.

  - Not all websites are RELIABLE because anyone can post anything online.
  Compare on-line information with books, other sites or people who know to make sure it's accurate/ true.
  You can pretend to be anyone you like online and so can the people you are chatting to as well. Learn how to block people who you think may be lying to you.

  - If something makes you uncomfortable or worried then TELL someone about it – someone you trust, an adult or friend. Use the CEOP report button.
  If you receive texts/ mails that upset you remember you don't have to reply. Or if you come across unsuitable content on a website that upsets you. Although you may want to delete them as quickly as possible, keep a record of them because they can be used as evidence.

Primary School age exemplar:

Think before you do

We can click on the buttons when we know what they do

We are always polite and friendly when we are talking to others on our phone or on the computer

We never give out personal information or passwords

We never do things that make us uncomfortable.

If someone asks us to do something rude, or something we don't like, then we tell an adult

We never arrange to meet someone we don't know

If we're not sure about anything then we ask an adult

E-safety rules for those working with children, young people, their parents or carers.

I appreciate that digital technology includes mobile phones, PDAs, digital cameras, games consoles and communication methods including email, social networking, instant messaging, twitter and blogs.

I will not disclose any password or security information that allows access to the network

I will not install any additional hardware or software without permission

I understand that the police will be involved if my use constitutes a criminal activity and the necessary disciplinary/ allegations processes may be invoked.

I will ensure that personal and confidential information is stored and transmitted securely in accordance with the information sharing requirements of this organisation.

I will not use my personal equipment for organisation business without permission from a senior manager.

I will promote e-safety with all children and young people I come into contact with in my role.

I will ensure that any electronic communications I may make with any child or young person, colleague or external professional, are compatible with my professional role. I will ensure that these messages are polite and respectful and cannot be misunderstood or misinterpreted.

I will act as an e-safety role model for all children and young people I come into contact with in my role.

I will report any incidents of concern, including unsuitable personnel, activity or content, to the E-safety lead and the Designated Child Protection Officer and the Senior Manager as appropriate.

I will make sure that any personal use of the system meets the AUP.

I will make sure that any personal social networking sites, email accounts etc. are set up securely. I will not allow access to my personal accounts to any child or young person I am working with in a professional role.

I will never pass on personal information about anyone related to my workplace to another person without their knowledge or consent

The organisation may exercise its right to monitor the use of information systems and internet systems, and to intercept email and to delete inappropriate materials where it believes unauthorised use of the systems may be taking place, or to maintain as evidence where the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Consent to e-safety rules exemplar

E-safety agreement

Child or young persons agreement

Name: Date of Birth:

☺ I have read and understand the e-safety rules.
☺ I will use the computer, mobile phones, internet access and any other digital equipment in a responsible way at all times
☺ I know that my behaviour and activity will be monitored.
☹ I understand that if I break the e-safety rules my equipment may be confiscated and my access to the network suspended. If this happens my parents will be informed.

Signed:
Date:

Parent or Carer's agreement

Consent for web publication of work and images
I agree that my child's work may be published electronically. I also agree that appropriate images and video that include my child may be published electronically providing that it does not identify my child by name.

Consent to internet access
I have read and understand the e-safety rules for this organisation. I give permission for my child to access the Internet. I understand that the organisation will take all reasonable precautions to ensure that my child is a safe and responsible digital user.
I understand that the organisation cannot be held responsible for the content of materials accessed through the Internet but I expect that the school will take appropriate action in accordance with the e-safety rules. I agree that the organisation is not liable for any damages arising from the use of digital technology.
I will support my child by demonstrating safe and responsible use of digital technology, including the use of social media.

Signed:
Date

Staff agreement

I have read, understand and accept the e-safety rules for those who work with children and young people, their parents or carers.
I will promote safe and responsible use of digital technology at all times.

Signed:
Date: