Where Children Come First'

Online Safety

Policy

The designated safeguarding lead is: Honoria Thompson
The online safety lead is: Sam Maddaford
The policy was agreed on: 13/06/2023
The policy will be reviewed on:13/06/2024

Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology, and provides safeguards and awareness for users to enable them to control their online experiences.

This policy will operate in conjunction with other policies including: **Child Protection and Safeguarding Policy, Behaviour Policy, Social Networking Policy, Computing Policy and Data Protection Policy.**

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 pupils 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's internet access will be designed for both staff and pupil use, and will include appropriate filtering because of this.
- Pupils will be taught what Internet use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Internet access will be planned to enrich and extend learning activities.

Pupils will be taught how to evaluate Internet content

- Internet derived materials by staff and by pupils must comply with copyright laws.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is part of every subject.
- Pupils will be taught how to report unsuitable Internet content.

Managing Internet Access

Information system security

- If pupils discover an unsuitable site, it must be reported to the class teacher who then is responsible for reporting to the school Online Safety Lead.
- If staff discover an unsuitable site, it must be reported to the Online Safety Lead
- Virus and Spyware protection will be installed and updated regularly.
- Login details must not be shared.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Email

- Pupils and staff may only use approved e-mail accounts in school.
- Pupils and staff must immediately tell a teacher if they receive offensive an e-mail.
- Pupils must not reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils and staff must treat e-mails with links or attachments as suspicious and not open any links unless they know they are safe.
- E-mails 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.
- The forwarding of chain letters is not permitted.
- Pupils will be taught how to report unpleasant internet content.

Published content and the school web site

- 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.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- A pupil's full name will not be used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

- The school's filtering system will block access to inappropriate social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Staff must not communicate with students using public social networking sites such as Facebook, Twitter, etc.

- Staff must not communicate with parents using public social networking sites such as Facebook, Twitter, etc. about school.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.

- The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy.

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.

Protecting personal data

- Personal data will be protected following the legal requirements of the Data Protection Act 2018.

Use of phones / mobile phones

- Staff must use a school phone where contact with parents/pupils is required.

- Staff will keep personal phones in their locker. They are not to be used in teaching sessions, but can be used in the staffroom at break times.

- Staff will not use their personal phone for photos or the Internet while in a teaching session.

- Pupils are not allowed a mobile phone in class. If they bring a mobile to school (which a parent must agree to) they have to leave it in a teacher's drawer at all times during the school day. There is a separate letter for parents to agree to this.

Policy Decisions

Authorising Internet access

- Pupils will be taught about the AUA. (Acceptable use agreement).
- All staff must read and sign the Staff Information Systems Code of Conduct before using any school ICT resource.
- The school's office manager will maintain a current record of all staff and pupils who are granted access to school ICT systems, which can be easily accessed by the school's online safety coordinator.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the size of the Internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access

Handling online safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- 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, should an issue arise.

Communications Policy

Introducing this policy to pupils

- Pupils will be taught about their age group's AUA. This will be displayed in classrooms.
- Users will be informed that network and internet use will be monitored.

Staff and this policy

- All staff will be given the school Online Safety Policy and have its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Filtering systems and monitoring of ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' attention can be drawn to the school's Online Safety Policy in newsletters and on the school website.

Online Safety Rules for Staff

These rules help to protect 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 the email could be forwarded to unintended readers.

- Anonymous messages and chain letters are not permitted.

- Users must take care not to reveal personal information through e-mail, personal publishing, blogs or messaging.

- The school's ICT systems may not be used for private purposes, unless the head

teacher has given specific permission.

- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

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

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the Online Safety Policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.

- I understand that the school may monitor my information systems and internet use to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.

- I will not install any software or hardware without permission.

- I will ensure that personal data is kept secure 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 incidents of concern regarding children's safety to the school's designated safeguarding lead.

- I will ensure that any electronic communications with pupils are compatible with my professional role.

- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

- I will not use social media to contact pupils from Shepton Mallet Community Infants' School & Nursery other than family members.

- I will not use social media to communicate with parents about Shepton Mallet Community Infants' School & Nursery.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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 agree with the Staff Information Systems Code of Conduct.

Signed: Date:

KS1 Accessible Use Access (AUA)

Acceptable Use Agreement

✓ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.

✓ I only open activities that an adult has told or allowed me to use.

✓ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.

✓ I keep my passwords safe and will never use someone else's.

✓ I know personal information such as my address and birthday should never be shared online.

✓ I know I must never communicate with strangers online.

✓ I am always polite when I post to our blogs, use our email and other communication tools.

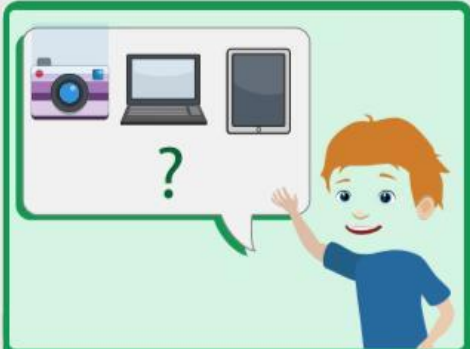**I understand this agreement and know the consequences if I don't follow it.**

My Name:

Class:

Parent/Carer Signed:

Today's Date:

Accessible Use Agreement EYFS (AUA)

Acceptable Use Agreement (For EYFS)

✓ I ask before I use a tablet, computer or camera.

✓ I tap or click on things I have been shown.

✓ I check if I can tap/click on things I haven't seen before.

✓ I tell a grown-up if something upsets me.

My Name:

Class:

Parent/Carer Signed:

Today's Date: