# The Winchcombe School

# Online Safety Policy

## We are committed to the safety and wellbeing of all our children

THE WINCHCOMBE SCHOOL POLICY DOCUMENT

| TITLE: **Online Safety** | STATUS: Recommended |
|---|---|

**Policy & Purpose**

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.

The school's online safety policy will operate in conjunction with other policies including Child Protection & Safeguarding, Behaviour and GDPR Policies.

**Teaching and learning**

Online Safety, Computing systems and networks and Data and information are strands within our Computing Curriculum. We have identified key knowledge for every year group, ensuring that children build on their understanding as they progress through the school. This knowledge is taught as part of every single Computing unit and is further embedded during PSHE lessons.

**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 and instruction 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 to enhance learning**

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils.

**Pupils are taught how to evaluate Internet content**

- Internet derived materials by staff and by pupils must comply with copyright laws
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Pupils will be taught how to report unpleasant 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 this by email to the TRI Computers Support desk.
- Virus and Spyware protection will be installed and updated regularly by the school's internet provider.
- 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 e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils and staff must treat emails with links or attachments as suspicious and not open any links unless they know it is safe.
- E-mail sent to an external organisation should be written carefully in the same way as a letter.
- The forwarding of chain letters is not permitted.

**Published content and the school web site**

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

**Publishing pupil's images and work**

- Pupils' full names will not be used anywhere on the school's web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.

**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.
- Pupils and parents will be reminded that all the major Social Networking sites require children to be older than Primary School age. However, we acknowledge that some pupils (with permission of parents) use Social Networking and therefore they should be advised on security. They are 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 or instant messaging services (e.g. WhatsApp) is difficult for staff to detect. Pupils will need educating that such use is both inappropriate and conflicts with school policy. Abusive messages may be dealt with under the school bullying policy.

**Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and an assessment of suitability will be carried out before use in school is allowed.

**Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR.

**Use of phones / mobile Phones**

- Staff should normally use a school phone where contact with parents/carers is required. However, personal mobile phones can be used to contact parents if the situation requires (e.g. during the COVID pandemic), in which case, the teacher's must hide their caller ID.
- Staff will usually keep personal phones in their bag or locker during sessions. If phones are needed during teaching sessions (e.g. to set reminder alarms) then they must be used solely for such purposes, and not for communication.
- Staff will not use their personal phone for photos or the internet while in teaching session.
- Pupils are not allowed a mobile phone in class. If they bring a mobile to school (agreed by parent) it is to be left in the school office and collected at the end of the school day. There is a separate letter for parents to agree this.

**Policy Decisions**

**Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, 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 headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. As such, any online safety incidents which affect individual pupils will be recorded using CPOMS.
- Pupils and parents will be informed of the complaint procedure.

| | |
|---|---|
| DATE: 7th January 2026 | REVIEW DATE: January 2029 |

SIGNED:

Head teacher 07.01.2026