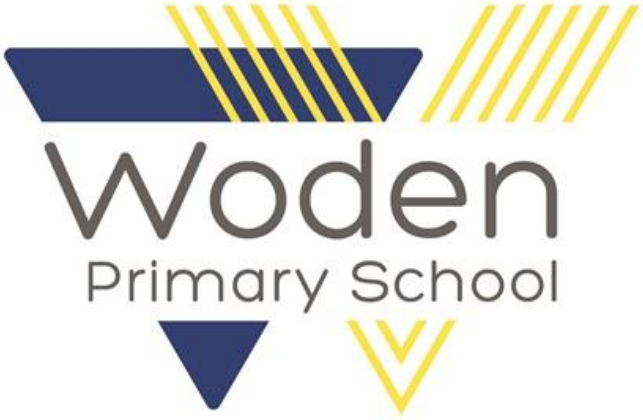
E Safety Policy



Primary Hub

2023-24

Writing and reviewing the e-safety policy

This policy has been developed to ensure that all stakeholders in the Primary Hub work to ensure safeguarding and promotes the welfare of children and young people. We aim to put effective management systems in place to maximise the education and social benefits obtained from ICT use whilst minimising the risks. This policy relates to other policies including those for ICT, behaviour and child protection.

Acceptable use of computers within schools is laid out in the schools Acceptable Use Policy separately.

Teaching and learning

Internet Access

- 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.
- Our internet provision will be filtered using the LA mediated filtering system.
- 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 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 shown how to publish and present information to a wider audience.
- 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 will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

E-mail

- When available, pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mails from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs that include pupils will be selected carefully so that individual pupils have had permission to be used.
- Pupils' names will not be used in association with photographs anywhere on the school Web site or other on-line space, unless permission has been given.
- Pictures and work will only be shown on the website if parents/carers have signed the consent form issued at the start of each school year.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- If they are to be used, the school will control access to social networking sites and consider how to educate pupils in their safe use.
- Currently we do not use social networking sites as part of the curriculum.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will use only moderated social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing videoconferencing & webcam use

- When available, videoconferencing and webcam use will be appropriately supervised for the pupils' age.
- Video conferencing equipment will always be shut off when not in use, kept securely and never linked to the school website.
- Conferences will only take place by prior arrangement and URL's will only ever be given to those taking part.

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.
- Staff 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.
- Mobile phones will not be used during lessons or formal school time by pupils.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR regulations.
- Whilst the transfer of data from home to school is inevitable, sensitive or personal data will not be taken home.
- Encrypted USB sticks will be used by pupils and staff.
- Logins and passwords will be kept private and where ever possible difficult to guess.
- Computers will be locked and encrypted when not in use.

Procedures

- The School ICT system's security will be reviewed regularly.
- Virus protection will be updated regularly.
- The school will work in partnership with parents, CLPT and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT helpdesk email address and the E-Safety Leader informed via email or verbal immediately
- ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- 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. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.
- Staff and pupils should be aware that internet traffic can be monitored and traced to the individual user.
- The monitoring system Impero will be used to provide detailed reports of any suspicious activity in

internet use. This will be provided to the Head teacher on a regular basis.

Discretion and professional conduct is essential.

- Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, email, instant messaging or telephone.
- Should special circumstances arise where such communication is felt to be necessary, the agreement of a line manager should be sought first and appropriate professional language should always be used.
- Staff must not use mobile phones during teaching time.
- Cyber-bullying will be dealt with using the schools behaviour protocols and is seen as a serious offence.

Prevention of radicalisation and extremism

The school's safeguarding policy covers Radicalisation and Extremism.

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism. Extremism is defined by the Government in the Prevent Strategy as: Vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs.

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 particular 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. 4. There 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.

The schools e-safety and safe use policies seek to set out how the school supports the aims of the Prevent Strategy by:

- Ensuring sufficient monitoring of internet access is in place to prevent access to violent and extremist websites, violent extremist literature and sites of extremist organisations
- Limiting access to social networking to prevent extremist recruiters and joining extremist organisations
- Sharing any relevant information in a timely manner with nominated child protection officers (Headteacher) using the school reporting forms

Handling e-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.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School E-Safety in the Home School Agreement; in newsletters and on the school Web site.
- The school will ask all pupils and staff to sign the relevant agreements at the start of each school year or when children are admitted in the case of in-year admissions.

If a child is at immediate risk

Consult with Leadership Team, Family and Child Liaison then Contact police (999) urgently if there is immediate danger.

Addendum: During Coronavirus Pandemic

Promoting online safety outside school

- School will ensure any online learning tools and systems used are GDPR-compliant.
- Staff should continue to follow the school e-safety and acceptable use policies
- Staff should continue to look out for signs that a child is at risk while they're not at school, including when interacting with them online. They should follow your policy for reporting concerns, and make referrals to children's social care and the police as needed.
- School staff behaviour policy and code of conduct still applies to any remote learning set. This covers acceptable use of technologies, staff/pupil relationships and communication, including the use of social media.
- Staff should ensure children know where to go with concerns, inform them of how to report back to school through the school office, year group email or Class Dojo, and make them aware of further sources of support, such as Childline, the UK Safer Internet Centre and Child Exploitation and Online Protection command (CEOP).
- Online safety information will be shared with parents and carers through the school website to reinforce the importance of children being safe online. Making sure they're aware of:

    - What we are asking their children to do online and what sites they'll be using
    - Who from your school will be interacting with their children online, if anyone
    - The importance of using reputable organisations or individuals if parents are getting additional support for their children (e.g. through online companies or tutors). They should be able to provide evidence of being safe to work with children
    - Resources that can help them keep their children safe online, like Thinkuknow, the UK Safer Internet Centre, London Grid for Learning, Net Aware, Internet Matters and Parent Info. If you're a member of Safeguarding Training Centre from The Key, take a look at our parent factsheets