

Woodcroft's *Online safety policy* relates to other Woodcroft School policies (such as the *Anti-bullying policy* and *Safeguarding children policy*), but specifically needs to be read in conjunction with the *Electronic information and communication systems policy*.

The term 'online' in this document refers to the internet and other forms of data transmission, such as tablets and mobile phones. All staff are made aware of this policy and its importance explained. A copy is available from the school office.

Internet and mobile phone use for children with SEN

Children with SEN are potentially more at risk and vulnerable than others when using ICT:

- Those children on the Autism Spectrum (AS) may make literal interpretations of content, which will affect how they respond.
- They may not understand some of the terminology used.
- Those with more complex needs may not always understand the concept of friendship and therefore trust everyone implicitly. They may not know how to make judgements about what information is safe to share, leading to confusion about who to trust online.
- Some children may be vulnerable to being bullied or exploited through the internet or via their mobile phone and may not recognize that this is happening.
- Some children may not appreciate how their own online behaviour could be seen by someone else as bullying.

Because of these increased risks Woodcroft has developed a set of *Internet and computer rules*, which are appended to this policy. Staff must follow these rules at all times and must encourage parents and pupils to engage with them at a level appropriate to each child.

Teaching and learning

The internet and mobile phones are essential elements in twenty first 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. It is also part of the statutory curriculum and a necessary tool for staff and pupils. We also have a responsibility to teach children about the safe use of communication technology, including the internet, mobile phones and social media.

Woodcroft School works to ensure that:

- School internet access is filtered and designed expressly for pupils use.
- Pupils are educated in the effective use of online technologies, through being taught what use is acceptable and what is not, and by being given clear objectives. Online safety rules are displayed in each classroom and discussed with pupils as part of their learning. Pupils are also informed that network and internet use is monitored.
- Pupils are taught how to report unpleasant online content to their teacher or parents.
- The school ICT systems, capacity and security are reviewed, and virus protection is updated regularly.
- The use of internet derived materials by staff and pupils complies with copyright law; and personal data is recorded, processed, transferred and made available according to the data protection legislation.
- Online safety training should be embedded within the ICT teaching and learning document and the Personal, Social and Health Education (PSHE) curriculum.

Notes:

- *The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.*
- *Woodcroft staff must not use personal email accounts or social networking applications to communicate with Woodcroft pupils or parents. Staff are provided with a school email address.*

Enlisting parent support

Parents co-operation with this policy will be sought right from the start of their child's enrolment at Woodcroft and this policy is also included in the *Parent handbook*. Parents' attention will be regularly drawn to the school *Online safety policy* via Parent newsletters and updated training and advice will be made available.

Mobile phones and tablets

Personal mobile phones are not used during lessons or otherwise at school, but mobile devices can be sent into school with pupils for use on transport. Pupils' personal devices are to be left in the school office and collected at the end of the day. (It is the responsibility of the pupils' parent to fit the correct filters on these personal devices.) Personal mobile devices **must not** be used to take photographs or videos of pupils. The sending of abusive or inappropriate messages is forbidden either by text or any other means. Visitors that have access to the classrooms may be asked to hand in their phones to the office manager. There are dedicated school mobile phones for all off-site activities.

Games machines

Games consoles with internet access are subject to the same filters as all computing devices within the school.

Email

Pupils are not given their own email accounts on the school system, but where appropriate, an approved email address for their use will be set up for curriculum purposes, which is monitored at all times by the class staff. Pupils will be taught not to reveal their personal details or those of others, or to arrange to meet anyone without specific permission.

Social media and personal publishing

The school will block or filter access to social networking sites using appropriate filtering software. Pupils are advised never to give out personal details of any kind which may identify them or their location. Pupils and parents are advised that the use of social network platforms outside school brings a range of dangers for our pupils. These risks are constantly changing as new apps and technologies are developed. The school will therefore endeavour to review its training regularly so that understanding of risks can be shared with colleagues, parents and pupils.

Managing filtering

Woodcroft reviewed its filtering and monitoring service in 2023 and decided to continue its use of the Smoothwall system. The system is overseen by our ICT technician. Unsuitable sites will be blocked, and flagged automatically to the head teacher. However, any unsuitable sites that are discovered by staff in addition to this, should be notified to the head teacher.

Managing emerging technologies

Emerging technologies will be examined for their educational benefits and dynamic risk assessment will be carried out before use in school is allowed. Staff 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.

Artificial Intelligence (AI)

AI will increasingly form part of the learning environment for our pupils. Whilst we recognise that there are potential benefits to AI enhanced searches and enhanced learning tools for some pupils, we also acknowledge risks to pupils and the school from these

emerging technologies. We acknowledge the four core areas of online risk identified in KCSIE: content, contact, conduct and commerce. In particular there are risks around the sharing of sensitive information; the presentation of bias or misinformation as fact; and the creation of obstacles to the natural development of original thought and authentic relationships.

As with internet searches, AI systems will sometimes provide biased or incorrect information. In the case of AI this can result from flawed or biased AI training models or commercial influences. In addition, AI systems can exhibit so-called 'hallucinations' where AI systems can replicate false or even maliciously introduced information, presenting this as fact. Our curriculum and home/school communications should therefore introduce pupils to age and ability appropriate digital skills. An individual pupil risk assessment on the use of AI avatars may be appropriate in some cases.

Staff will be trained to help pupils critically evaluate online information and report anything that causes concern. Staff and, through them, pupils will be made aware that AI content may be inaccurate, biased or inappropriate and any AI outputs will be checked by a responsible adult. Incidents involving AI use will be logged and addressed under safeguarding and behaviour policies.

The school's IT technical support service should be consulted regularly to ensure blocking of known unsafe AI tools and the support of approved AI tools, where used.

Woodcroft has developed a set of rules for AI based systems which takes into consideration the specific learning needs of our pupils:

- Pupils should be encouraged to develop their own thinking and analytical skills and to use these before reaching for AI tools.
- AI systems are not to be used instead of, or to supplement, personal face-to-face teaching.
- Pupils should be advised of the potential of inaccurate, biased or inappropriate content.
- Pupils should not be allowed to become dependent on AI or single source searches for verification of information or to replace natural intellectual processes.
- We recognise the challenges that some of our pupils have in developing and maintaining relationships and need to be aware that seemingly real interactions with AI based avatars or programmes may be attractive or addictive.
- Staff should make themselves aware of the differences between regular and AI based learning tools and should ensure that pupils who can understand the difference are also informed about this.
- No personal data, e.g. staff or pupil information, EHCP data or assessment data, is to be put into AI systems.
- Information that is the property of the school should not be put into AI systems, as this may breach confidentiality or copyright rules.

Published content and the Woodcroft School website

Contact details on the school website include the school address, email and telephone number. Staff, parents' or pupils' personal information will not be published. Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified. Pupils' names should not be used anywhere on the public website. Written permission from parents for the use of photographs on the website is sought prior to use.

Handling online safety complaints

Incidents of inappropriate internet content will be reported to the head teacher, who will liaise with the online safety coordinator. These incidents will be logged by the head teacher. Incidents of a safeguarding nature must be dealt with in accordance with the school's *Safeguarding children policy*.

Internet and computer rules Woodcroft School 01.11.25

It is the responsibility of all staff to ensure that these rules are followed in order to protect pupils, staff and the school as a whole. These rules form part of the school's *Online safety policy*. Please note that breaches of these rules will be deemed as misconduct and could lead to disciplinary sanctions, up to and including dismissal for gross misconduct.

- **Pupils must never be allowed to use internet-enabled mobile devices or computers unsupervised.**
- **Only pre-checked live sites and searches or offline sites may be used during pupil sessions.**
- **Pupils should be told of the potential for inaccurate, biased or inappropriate online content, including that generated by Artificial Intelligence (AI).**
- Pupils should be encouraged to develop their own thinking and analytical skills and to use these before reaching for AI tools.
- AI systems are not to be used instead of, or to supplement, personal face to face teaching.
- Pupil internet sessions must be planned for alongside the individual pupils' learning goals, and risk assessments must be carried out.
- The school uses Smoothwall to provide part of the schools internet filtering and monitoring service. However, new threats can be introduced at any time, so the assumption is that staff will provide the final safety checks.
- Internet and network access must be made via the user's authorised account and password, which must not be given to any other person.
- School computer and internet use must be for pupil education or staff professional activity only, subject to the *Electronic information & communication systems policy*.
- Pupils are not permitted to use email, social media or chat rooms.
- No pupil or staff personal data or information concerning the school should be put into AI systems.
- The school may monitor the use of its computer systems by, for example: monitoring access to websites; intercepting email; and viewing files stored on computer. It may do this for reasons including but not limited to: enforcing the above rules; where it believes unauthorised use may be taking place; or where it believes the system may be being used for criminal purposes.