Online safety Woodcroft School pupil policy 01.11.23

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

Personal mobile phones are not used during lessons or formal school time, but mobile devices can be sent into school with pupils for use on transport. (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.

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

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 are taken from the school's *Online safety policy*, which is available from the office.

- **Pupils must never be allowed to use the internet or mobile devices unsupervised.**

- Pupil internet sessions must be planned for alongside the individual pupils' learning goals, and risk assessments must be carried out.
- Only pre-checked and/or 'walled garden' sites may be used during pupil sessions. (The school uses Smoothwall filtering and monitoring to provide the schools internet safety service.)
- Pupils are not permitted to use email, social media or chat rooms.
- School computer and internet use must be for pupil education or staff professional activity only, subject to the *Electronic information & communication systems policy*. The school computer systems may not be used for private purposes, unless the head teacher has given special permission for that use.
- Internet and network access must be made via the user's authorised account and password, which must not be given to any other person.
- Staff emails should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers. Staff are responsible for emails they send.
- Copyright and intellectual property rights must be respected.
- Chat rooms, anonymous messages and chain letters are not permitted.
- Irresponsible use may result in the loss of internet access or disciplinary action.
- Computer security must be respected.
- 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: to enforce 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.