# FOX WOOD SCHOOL

# ONLINE SAFETY POLICY

Headteacher: Miss Lucinda Duffy

Fox Wood School
Woolston Learning Village
Holes Lane
Woolston
Warrington
WA1 4LS

Tel: 01925 811534

Review Date: November 2028

Date: November 2025

**The use of the internet at Fox Wood School is a privilege.**

## Philosophy

We at Fox Wood School believe that teaching and learning can be greatly enhanced for our pupils through the use of Computing and the internet. We feel that Computing is also important to our staff, as a teaching and learning tool and as a means of training. This internet policy has been drawn up to protect all parties – pupils, staff and the school.

Online Safety is taken extremely seriously by all staff.

## Aims

1. This Online Safety policy should be read in conjunction with our Computing Guidance.
2. All teachers have a school e-mail address. Use of their own personal email accounts is permitted but school business should be dealt with on the official email account.
3. The internet is used by staff and pupils for educational and communication purposes.
4. The internet may help our pupils to increase their independence and help to develop their ideas and interests.
5. This policy is compiled in consultation with staff, parents and governors.

Fox Wood school encourages the use of Computing (including Computer Science, Information Technology, Digital Literacy and the Internet and Email) in a responsible way, in order to enhance pupils' experience and raise standards. Staff and Governors have access to the School's Computing system to support these aims, (including Internet and Email), subject to a written undertaking to abide by this Code of Conduct. Pupils have access to Internet and Email facilities upon acceptance of the Computing code of conduct for pupilsThe Governing Body recognises that the development of staff expertise relies on frequent use of these technologies. Therefore, subject to considerations of cost and considerations of "abuse" staff are permitted to use the School's Computing facilities for personal use, subject to agreement in individual cases by the Headteacher or Senior Leadership Team. (This permission may be withdrawn without alteration to this document, if circumstances change.) All staff should be aware that the school Computing equipment has security monitoring software called Securus. The use of mobile phones when working with pupils is also prohibited, unless agreed to by the Senior Leadership Team on a very rare occasion if the need arises..

## Computing Provision

### Physical Safety

- All electrical equipment in the school is subjest to “PAT” testing (portable appliance testing) and is tested regularly to ensure that it is safe to use.
- Workstations are cleaned and sanitised regularly. Pupils are taught to avoid taking food and liquids anywhere near the computers. We expect all users to refrain from eating and drinking when working at a computer
- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. Comfort of pupils is taken into account when setting heights of rise and fall tables and peripherals required by our pupils with Profound and Multiple Learning Difficulties. We expect all users to take responsibility for their own physical well-being by adopting good practices.
- Computers and other Computing equipment can be easily damaged. We expect staff and pupils to respect Computing equipment taking care when handling and using staff must also ensure they report any damage.

### Network Safety

All users have an individual log on using a username and password.

- From staff assessment, some pupils (usually formal learners) have a log in with a full username and password. Other pupils will log on using only initials. (pupils may require 1-1 Physical/verbal support to do this.)
- All staff have their own log ons.

**We expect all users to only logon using their username.**

- Staff are asked to lock their workstation when they are not working on it to maintain their own security.
- The above is monitored by spot visits by the Computing Lead and Safeguarding Team and reported back to the DSL and the relevant staff

## Filtering and Monitoring

Schools should provide a safe environment to learn and work, including when online. Filtering and Monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. Fox Wood School have effective and well managed Filtering and Monitoring systems in place.

### Filtering

At Fox Wood School we use Smoothwall to provide an effective, appropriate and reasonable filtering system which blocks internet access to harmful sites and inappropriate content.

The filtering is set up for specific user groups e.g teachers and pupils. It does not negatively impact teaching and learning or restrict pupils from learning how to assess and manage risk themselves.

No filtering system can be 100% effective; however, the implementation of this policy ensures that the school filtering system is blocking access to illegal child sexual abuse material, unlawful terrorist content, offensive language and adult content. Staff know how to report and record concerns. Changes and updates are shared with all staff as part of their regular child protection training and as ongoing updates through Safeguarding Bulletins and in staff meetings.

Staff know that they should report if:
• They witness or suspect unsuitable material has been accessed.
• They can access unsuitable material.
• They are teaching topics which could create unusual activity on the filtering logs.
• There is failure in the software or abuse of the system.
• There are perceived unreasonable restrictions that affect teaching or administrative tasks.
• They notice abbreviations or misspelling that allow access to restricted material.

**Monitoring**

**The school has monitoring software on all Computers and Laptops (Securus).**

Securus detects inappropriate content as soon as it appears on screen, whether it has been typed or received by the user. A screen capture is taken of every incident, showing what was displayed at the time, who

was involved and when the incident took place. This software was designed by the police and records all use of Computers and cannot be removed once installed. Laptops also have this software and when they attach to the school network any Securus logs are automatically uploaded to the Securus server. The system creates security logs which if a threshold is met sends an email to the Safeguarding Team. Securus is monitored by the DSL and UTL to ensure it is working correctly.

- All staff and users or appropriate adults (for students) are aware of the securus program and have signed the Computing code of conduct.
- Each user is given a “Home drive” (My documents). Where appropriate Pupils are taught how to save their work into their “Home drive” area. We help and support pupils to save and keep their work to build up a portfolio of evidence.
- Access to other users “Home drive” areas are restricted by the network. Users are taught not to access another user’s work without permission. We expect users to respect the privacy of all other users and to make no attempt to access or interfere with another user’s work.

- On the network there are “shared resource” areas where many different groups of users can save work so that it is available to others. Users are taught how to access and save to these shared resource areas. We expect users to respect the contributions of others, not to delete or alter others’ work and to ensure that they only save work to shared areas with permission. Confidential data or data we do not wish to be edited is ‘read only’.
- Checks to the filtering and monitoring provision are completed and recorded monthly by UTL and shared with the DSL. Block lists are reviewed frequently and can be modified in line with safeguarding risks. UTL ensures that the filtering and monitoring system works on new
- devices and services before these are released to staff and pupils. Pupils are not
- allowed to use mobile phones to access the internet in school. This ensures that all access is via our filtering and monitoring system.

- Printing is not at the moment restricted. Users are taught to only print when necessary to save resources for financial and environmental reasons.
- The network software prevents changes being made to computer settings.Users are taught that making changes may prevent the computer from working properly.
- Only the network administrators are permitted to install software on to computers.
- All users of the network can be monitored remotely by the network administrators. We expect all users to understand that their use is subject to monitoring.

**Internet Safety**

- When using a network workstation all access to the Internet is protected by the filtering and monitoring systems detailed above. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually add site addresses which are considered to be unacceptable. However, no system is 100% safe and we expect users to behave responsibly. Users are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly and that some sites can damage your computers. We monitor all access to websites that may be unsuitable for children and/or containing offensive language, images, games or other media.
- Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet. We do not allow staff to “friend parents or pupils” on facebook. If they are approached they must inform the school SLT team immediately.

- We participate in an Online Safety day in February each year.
- All pupils participate in writing their own Online safety rules as appropriate to age and ability.
- We offer personalised support to parents and carers on online safety at home, this might be through 1:1 meetings, support offered through Annual Reviews/Parents Evenings or by providing fact sheets and handouts about different apps/games.

**School Website /www.foxwoodschool.org.uk)**

- Each class has access to the school website.
- It contains school policies, newsletters and other information. The website is managed by a group of staff and SLT. This group includes the Computing Co-ordinator, the TA for Computing and one member of the admin team.
- Photographs are only displayed with parental permission and pupils names will not appear in full. We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.

**E-mail Safety**

- An e-mail facility is provided for pupils and staff to make contact with other pupils, staff or establishments. Pupils may use their pupil email under supervision from a member of staff. E-mail accounts are set up for the intended user only. Unauthorised use of other people's accounts to send and receive e-mail is unacceptable.We expect all users to communicate in an appropriate manner through email.
- Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore we do not permit the use of personalised email accounts by pupils at school or at home for school purposes.Pupils are taught that using a personalised webmail account in school or for school use is not permitted.We expect pupils to use school issued email accounts only whilst in school.
- Whilst staff are allowed to access their own home/personal email accounts in school, they are aware that all access is monitored by "Securus", also that it is limited to break times or before or after work.

**Use of Digital Images**

Please refer to the Data Protection Policy

- Pictures of pupils or visitors are not allowed without consent of an appropriate adult

- Digital still and video cameras are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction, parents are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website. When images of pupils are used on the school website or social media their full name is never used. The school will remove any image of a child on the school website or social media pages at their parent's request.
- Staff are not permitted to use their personal mobile phones in school when pupils are present. The only exception to this is when mobile phones are needed for education led activities and this is agreed with SLT or when out on an educational visit and it is needed to make contact with school/a parent/emergency services.
- Pupils and staff must not take photos of pupils using mobile phones.

## Home/School Links

Extending Computing experiences at home is both valued and encouraged. Parents/carers are asked for their permission for our pupils to use the internet and comply with our conditions of use (see attached Conditions of Use document.) Parents have been invited to attend Family Learning sessions in school including Computing training and are requested to sign Fox Wood's Conditions of Use document.

Parents are offered the chance to discuss appropriate Computing equipment used by their son/daughter in school eg. access devices, and can attend sessions where they are shown how to use these and where to obtain such items should they be interested.

## Conditions of Use

The internet is available to staff, pupils and governors and other invited persons under the following conditions.

A copy of these conditions is distributed to all users and parents/carers, they sign and acknowledge acceptance of the conditions. A copy of these conditions will also be available in every class and in the staff room.

## Staff

- All members of staff are responsible for explaining the rules and implications of possible misuses of the internet and their responsibilities towards the pupils.
- Staff using the internet in school will be required to sign a copy of the" Code of conduct".

- Fox Wood school staff are required to connect their staff laptops to the school network at least once a week during term time to ensure antivirus and updates are carried out

All staff whether part time, full time, teaching staff or non teaching staff are allowed access to the internet in accordance with the following provisions.

All internet use shall be for the purpose of:

- Looking for information so that pupils or staff may gain a better understanding of a subject.
- For staff training purposes where the information is available via the internet.
- The use of e-mail for contact with other businesses or establishments on school business or to request information for the benefit of the school.

The internet should be used in a professional manner. Internet use using the World wide web (WWW) and internet phone and fax services shall be for school purposes only unless with consent of the headteacher.

All staff members receive training on how to access the school website.

## Pupils

Pupils shall be able to use the internet under the following conditions:

- The code of conduct will be adhered to by all pupils who use the internet within the school
- The internet is provided for the education of and the improved delivery of curriculum material(s). Pupils are encouraged to make use of the services to this end.
- pupils are not allowed unsupervised access to the internet, a staff member is always in the room. We also have Securus, our monitoring software,, on all machines which alerts SLT to possible misuse.

## Online Safety for pupils with additional educational needs

Our pupils at Fox Wood have a range of Special Educational Needs and require additional support to safeguard themselves.

- Some pupils may need additional teaching that includes reminders and explicit prompts of how to keep safe when using the internet.
- Visual support is important to aid pupils' understanding and pupils may respond well to multi-media presentations of Online Safety rules, such as interactive power-point slides, sounds and recordings.

- Many of our pupils have limited social understanding which may leave them open to risks when using the internet individually and also with peers. Adults need to plan group interactions carefully when raising awareness of internet safety. (this is extended to support within the home environment if requested)
- Some of our pupils choose recreational internet activities that may be aimed at pupils younger than themselves. By their very nature, these activities tend to be more controlled however staff need to plan how to manage pupils who may want to do the same as other peers but who may need small step teaching due to limited experiences with internet use.

## General statement

The School's SLT and the Governing body reserve the right to make random audits of the history files that record which web sites pupils and staff have visited. This is easily facilitated by "Securus".

- Staff accessing inappropriate sites will be dealt with through the school disciplinary policy.
- If pupils are found to be accessing inappropriate sites, parents will be informed and strategies will be put in place to ensure it doesn't occur again. This may include 1-1 only accesss to ICT or symbol based rules depending on ability and understanding.
- Removeable storage devices not specifically for school business should not be used on the school network

## Use of service

- No profanity or obscenities are to be used in any e-mail messages. We use RM Easymail and this does restrict swearing etc and an email is sent to the webmaster if rules are violated. This is then passed to the schools SLT.
- No private information is to be distributed to other parties at any time. This includes reposting of information sent by another party.
- The network is not to be used by any member of staff or pupils for personal gain or illegal activity.
- Deliberate attempts to gain access to WWW containing material of pornographic, racially or religiously offensive or illegal material will be dealt with as a serious breach of school rules.
- Downloading of material must be scanned for viruses at all times and any deliberate attempt to spread viruses through the network will be seen as a breach of the guidelines and dealt with as such.
- All copyright, privacy and international laws are to be abided by at all times.

## Liability

Fox Wood School is not, and cannot be held responsible for the loss of material, accidental corruption or any other action that might affect transmission or loss of data.

Fox Wood School has taken all possible precautions to maintain the safety of all users and these guidelines are written and enforced in the interest of all users' safety and effective use of the internet. Smoothwall filters all internet access into the school. Fox Wood also has an additional firewall for further protection. Through the curriculum in school all staff will guide our pupils towards the appropriate materials. Staff will not knowingly set pupils homework where the topics of research would lead to unsavoury sites and staff will visit suggested websites for viability before any lesson is undertaken.

Outside of school, families have responsibility for guiding their child's use of the internet, although Fox Wood communicates with parents and carers to reinforce safe procedures at home. School will support pupils to gain a basic understanding of Online Safety that is age and stage appropriate.

## Abuse of the guidelines

Those staff who abuse these guidelines will be dealt with accordingly. Please see the "Computing Code of Conduct"

**In all cases of abuse the police and/or the local authorities may be involved.**

## Summary

We have in place filtering, monitoring and management systems to protect the interests of management, staff, pupils and parents. The policy will be reviewed regularly.

The following documents were consulted in reviewing this policy:

- Warrington Borough Council guidelines
- 360 E-safety

Research was also conducted via the internet.