WOODSIDE SCHOOL

Online safety policy for Woodside School

Independent School Standards: paragraphs 7 and 34.

Policy content includes:

- our use, filtering and monitoring of the internet
- our commitment as 'phone-free' schools
- how we manage and store personal data
- how we manage online safety incidents.

This policy pays regard to the latest 'Keeping Children Safe in Education' (September, 2024) statutory safeguarding guidance, and the DfE's 'Teaching online safety in schools' guidance (June, 2019).

Last external review	September 2024
Next external review	September 2025
Latest update	September 2024

INTRODUCTION

We recognise that pupils' use of the internet is an important part of their education but that there are risks associated with its use. It is a prevalent issue; staff recognise that a lot of our pupils are extremely vulnerable and require a lot of guidance. We work closely with our safer schools' officer, and teach online safety across the curriculum. The DSL takes lead responsibility for online safety, ensuring that all staff understand and are aware of the filtering and monitoring systems in place across the schools.

This policy is based on the DfE's 'teaching online safety in school' guidance (June, 2019) and the DfE's filtering and monitoring standards. It addresses how we seek to minimise these risks in our schools and teach pupils how to stay safe when using the internet at home and outside of school.

We also recognise that all members of staff must always be mindful of the need to follow our policy of acceptable use of our IT equipment.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside of school. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of our wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote achievement.

Unfortunately, the use of these new technologies can put pupils at risk within and outside the school; pupils are not allowed to have any mobile device on them during the school day; this helps to safeguard pupils and ensure they are not accessing any inappropriate material on their personal devices.

We have a filtering system provided by Fortigate, which prevents pupils from accessing harmful and inappropriate content. We also have a pro-active monitoring system, provided by Senso, which allows us to monitor all internet use and provides information such as violations and blocks, as well as urgent notifications when a pupil attempts to access or search for harmful and inappropriate material. This is in addition to physical monitoring by staff supervising screens of pupils and live supervision managed via a console through Senso. The software systems we use provide weekly reports and the system is regularly reviewed to ensure we have effective monitoring strategies in place to meet the needs of the schools. While filters should not over block, as it may place unreasonable restrictions on what pupils can be taught, it is also fundamental to be aware of some of the potential dangers that the internet can pose, including:

- Access to illegal, harmful or inappropriate images, video games or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming

- The sharing/distribution of personal images without an individual’s consent or knowledge

- Inappropriate communication/contact with others, including strangers
- Sexting
- Implications of geolocation (being able to track someone's location via a mobile phone
  or internet-connected computer)
- Cyber-bullying
- Harmful online challenges and online hoaxes – see further guidance
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- The potential for excessive use which may have a negative impact on the social and emotional development and learning of the young person.

Teaching pupils about the safe use of technology is embedded throughout the curriculum and pupils are taught about online safety and risks as part of a whole school approach. Staff know to report and log any online safeguarding concerns via our online safeguarding portal and to the DSL.

This policy also pays regard to the government guidance issued by the UK Council for Internet Safety https://www.gov.uk/government/organisations/uk-council-for-internet-safety and should be read in conjunction with our 'keeping our pupils safe', 'healthy living (RSE)' and 'anti-bullying' policies, including staff discipline, conduct, capability & grievance procedures.

THE INTERNET

We have a duty to provide pupils with quality internet access as part of their learning experience. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for its use. All staff involved with teaching and learning will prepare pupils to benefit safely from the opportunities presented and ensure that they have a growing understanding of how to manage the risks involved in online activity in the following ways.

- Discussing, reminding or raising relevant online safety messages with pupils routinely, wherever suitable opportunities arise

- Reminding pupils, colleagues and parents/carers about their responsibilities, which have been agreed through the User Agreement (Appendix 1) that all pupils and parents/carers have signed

- Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. Access levels will also be reviewed to reflect curriculum requirements

- Teaching pupils as a planned element of personal, social, health, economic and citizenship and computing education about online safety, cyber-bulling, misuse of technology, the law in this area and how to correctly use modern technology for positive reasons.

MANAGING AND SAFEGUARDING COMPUTER SYSTEMS

The schools commission IT consultants whose responsibilities include ensuring the

personal

safety of staff and pupils in terms of our IT provision. It is also the IT consultants' role to work with the leadership team to ensure that the security of the schools' systems and its users are reviewed regularly. To support the maintenance of the schools' IT system:

- Workstations are secured against user mistakes and deliberate actions
- Our servers are located securely and physical access is restricted to appropriate staff
- The server operating system is secured and kept up to date
- A firewall is maintained and virus and malware protection for the whole network is installed and current
- Virus protection is installed and current on all laptops used for school activity
- Access by wireless devices is proactively managed (pupils cannot access the school's wireless network unsupervised)
- Portable media may not be used without specific permission followed by a virus check
- Unapproved software is not allowed on any school machines
- Files held on the schools' network are regularly checked
- IT consultants will review system capacity regularly
- Any administrator or master passwords for school IT systems are kept secure and available to at least two members of staff, e.g. the CEO, EP and DSL. The password is changed regularly to maintain a high level of security.
- No-one except the IT consultants, the CEO, EP or DSL is allowed to download and install software onto the network
- New users can only be given access by the IT consultants, once permission is given by a member of the leadership team
- Any laptops or school technology taken off school sites must be used in accordance with this and all other relevant school policies and any damage or loss is at the expense of the staff member.

MONITORING AND FILTERING INTERNET ACCESS

- As mentioned above, the internet usage at our sites is filtered and monitored by a system called Fortigate. This allows the DSL and members of the leadership team to check pupils' internet usage at the three sites. Our IT consultant and the DSL receive alert notifications and weekly

summaries of activity from Senso and are able to immediately filter information in order to highlight potentially concerning activity and identify the user involved. The advanced filtering and monitoring made available to us by Fortigate and Senso goes above and

beyond that which is mandated in the latest 'Keeping Children Safe in Education' statutory guidance and the DfE 'Teaching online safety in school' guidance

- Our site's internet is filtered through LGFL servers. It is not currently possible to employ Fortigate's monitoring system at Vauxhall, so staff are required to be extra vigilant in monitoring pupils when using any internet-capable device

- The wireless network is secure and is password-protected, which prevents unauthorised access. All users will be required to enter their username and password before being able to access the network from any device

- Staff have access to administer/download PCs and laptops that are part of our domain and they have LOCAL ADMIN access only

- A firewall is installed on the schools' networks, which provides web/content filtering, ensuring that reasonable precautions are taken to prevent access to inappropriate material. However, it is not always possible to guarantee that access to unsuitable material will never occur

- Teachers are encouraged to inspect websites they wish to use beforehand and will be responsible for all pupils who access the internet in their lessons

- Additional filtering may be installed by the schools as and when required

- All users are informed about what to do if inappropriate material is accessed or found on the computer.

NETWORK ACCESS

There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary login.

- All users are provided with a log-in appropriate to their role within the schools

- Pupils are taught about safe practice with regard to login and password information

- All passwords are changed termly to maintain a high level of security

- Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information

- Remote access to school systems is limited and covered by specific agreements and is never allowed to unauthorised third-party users

- Guests or non-WS staff are not given the Wi-Fi password unless a guest login is available.

EMAIL

- Email is regarded as an essential means of communication and all employees are provided with an e-mail account. Communication by email from teaching staff and administration staff to parents/carers and to external organisations should be related to school matters only. Email messages related to school matters should reflect a suitable tone and content, ensuring that the good name of the schools is maintained.

- The same procedures are expected of all other employees who send emails to external organisations and colleagues.

- Use of the schools' e-mail system is monitored and checked and staff should not use personal email accounts during school hours or for professional purposes. Staff are not permitted to use school email accounts to communicate with pupils at any time.

- See our data protection policy for further information on use of email and storing documents on Google Drive.

PUBLISHING MATERIAL ONLINE AT WS.UK

- Woodside Schools maintains editorial responsibility for website content to ensure that the content is accurate and the quality of presentation is maintained. The schools maintain the integrity of their website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

- The identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the website unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs never have names attached.

Pupils publishing online (blogs and websites)

- In some instances, it may be appropriate for pupils to use websites or blogs to complete, or celebrate, their work. As always, the identities of pupils must be protected at all times. Photographs of identifiable individual pupils are not published unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs must never have full names attached (first name or initials only) and no personal information that could be used to identify them should be disclosed. Parents/carers must have given specific permission via the user agreement forms to allow pupils to create websites or blogs.

Other online communication platforms

- Staff and pupils are encouraged to adopt similar safe and responsible behaviour in their personal use of blogs, wikis, social networking sites and other online publishing inside and outside of school hours. Material published by pupils and staff in a social context which is considered to bring the schools' reputation into disrepute or considered harmful to, or

harassment of, another child or member of the organisation will be considered a breach of conduct and behaviour and treated accordingly, as per

our behaviour, equality, anti-bullying and/or staff conduct policy/procedures.

USING IMAGES, VIDEO AND SOUND

- Woodside Schools recognises that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are encouraged and taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

- Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

- All parents/carers are asked to sign an agreement about taking and publishing photographs and video of their pupils when offered a school or activity placement and this list is checked whenever an activity is being photographed or filmed.

- For their own protection staff or other visitors to our premises are discouraged from using a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils or visitors.

MOBILE PHONES

- Pupils are discouraged from bringing mobile phones into school but if they do they must hand them to the school offices for safe keeping until the end of the school day. School staff are not to use mobile phones during the school day, with the exception of calling the school or the emergency services if an emergency situation arises whilst off-site (e.g. school trips). Staff are not encouraged or expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a child or parent/carer. Unauthorised or covert use of a mobile phone or other electronic device, to record voice, pictures or video is strictly prohibited.

- The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, ‘cyber-bullying’, will be considered a disciplinary matter for pupils and staff alike. The same is the case for other inappropriate use of mobile technology, such as ‘sexting’. Pupils are taught about misuse of technology as a matter of course through the school’s personal, social, health, economic and citizenship education programme. See our ‘what we teach’ policy for curriculum information.

NEW TECHNOLOGY

- Woodside Schools will keep abreast of new technologies and consider

both the benefits for learning and teaching and also the risks from an online safety point of view. We will regularly review this policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

- Employees, visitors or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

DATA (SEE OUR DATA PROTECTION & CONFIDENTIALITY POLICY)

The schools recognise their obligation to safeguard staff and pupils' personal data including that which is stored and transmitted electronically. We ensure:

- Pupils are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties

- Staff are provided with appropriate levels of access to the schools' management information systems (ScholarPack) which holds child data. Passwords are not shared and administrator passwords are restricted and kept securely

- Staff are aware of their obligation to keep sensitive data secure when working on computers outside of school

- When we dispose of old computers and other equipment, we take due regard for destroying information which may be held on them

- Remote access to computers is restricted to teachers & leaders

- There is full back up and recovery procedures in place for school data (all pupil and staff data is kept securely in the 'cloud' online)

- Where sensitive staff or child data is shared with other people who have a right to see the information, for example professionals in social care teams, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

- All staff sign a contract which includes a confidentiality section when commencing work at Woodside Schools

- Please refer to our data protection policy.

ONLINE SAFETY INCIDENTS

- All incidents, including online safety incidents, are recorded as per other incidents on our online data management system, ScholarPack.

- Any incidents where pupils do not follow the User Agreement will be dealt with following the school's behaviour policy and procedures.

- In situations where a member of staff is made aware of a serious online safety incident, concerning pupils, visitors or staff, they will inform a senior leader who will respond in the most appropriate manner,

according to the flowchart in Appendix 2.

- Instances of cyber-bullying will be taken very seriously and will be dealt with using the schools' preventing and responding bullying procedures and the organisation's disciplinary procedures. The organisation recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

- Incidents that create a risk to the security of the schools' network, or create an information security risk to the organisation, will be referred to the CEO. Appropriate advice will be sought and action taken to minimise any risks and prevent further instances occurring, including reviewing any policies, procedures or guidance.

- If the action breaches school policy, appropriate sanctions will be applied. The schools will decide if parents/carers need to be informed if there is a risk that child data has been lost.

- Woodside Schools reserves the right to monitor their premises' equipment and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

GOVERNANCE

The Education (Independent School Standards) Regulations apply a duty to proprietors of independent schools to ensure that arrangements are made to safeguard and promote the welfare of children. Woodside Schools is led by a proprietor body, supported and held to account by external members of the quality & standards committee. The proprietors ensure that they comply with their duties under legislation and fulfil their duty to remedy any weaknesses that are identified.

In relation to online safety, duties and responsibilities include:

- The DSL has a termly meeting with a designated member of the quality & standards committee, Barney Payne, who is responsible for ensuring effective safeguarding practices and compliance with the relevant ISS, including in relation to online safety and the effectiveness of the schools' filtering and monitoring systems, making sure that the 'Filtering and monitoring standards for schools and colleges' guidance is met in full.

- The proprietor and the members of the quality & standards committee ensure that appropriate filters and monitoring systems are in place, across all of the schools' sites, to ensure that pupils are safeguarded from potentially harmful and inappropriate material. Their effectiveness is regularly reviewed, at least annually, in collaboration with the schools' IT consultants and DSL (who takes lead responsibility for filtering and monitoring). These termly reviews thoroughly consider whether the current filtering and monitoring systems are meeting the needs of the schools and whether any action is required.

- The proprietor and the members of the quality & standards committee

ensure that pupils are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.

FURTHER ONLINE SAFETY SUPPORT AND INFORMATION

Please refer to Annex B of 'Keeping Pupils Safe in Education' (September, 2024) as it provides a wealth of information, advice and support for families on online safety, including links to a range of organisations.

PUPILS' ONLINE ACCESS OUTSIDE OF SCHOOL, INCLUDING REMOTE USE OF GOOGLE CLASSROOM

- Teachers are in regular contact with pupils' families. This communication is used, as necessary, to reinforce the importance of keeping their children safe online.
- Teachers may use Google Classroom as an online learning platform for the setting of work and for facilitating remote education. Our remote education provision reflects the NSPCC's helpful advice, 'Undertaking remote teaching safely'.
- We acknowledge that families are likely to find it helpful to understand what systems we use at WS to filter and monitor online use. Teachers ensure that pupils' families are aware of what their children are being asked to do online in school and remotely, including the sites they are asked to access and who their child is going to be interacting with online.

Appendix 1: Pupil User Agreement

WOODSIDE SCHOOL

PUPIL COMPUTER & INTERNET

USER AGREEMENT

THIS MUST BE SIGNED BY BOTH PUPIL AND PARENT/CARER BEFORE INTERNET ACCESS IS ALLOWED

At Woodside School, we expect all pupils to be responsible for their own behaviour on computers and the internet, just as they are anywhere else in school.

Where applicable, this is to be read through with your parent(s) and then signed. You will be allowed internet access after this is returned. These rules will keep you safe and help us be fair to all.

General Computer Use

- I will only access the system through the proper log-in and will keep my password secret from others
- I will not access other people's files
- I will only use the computers for school work and homework
- I will not use rude language in my

work Internet User Agreement

- I will ask permission from a member of staff before using the internet
- I will not download any files from the internet
- I will not try to access social media sites or instant messaging services
- I will not email people unless teachers approve it
- I will never give out my personal details online
- If I see anything rude, or anything that worries or upsets me, I will tell a teacher immediately
- I understand the school may check my computer files and internet usage
- I will only use approved websites and all communications will be supervised and appropriate
- I know that if I break these rules, I may lose access to the computers and internet in school

AGREEMENT/PERMISSION FOR INTERNET ACCESS – SIGN HERE	
Pupil	Parent/carer (if applicable)

I agree to follow the rules for responsible internet use Sign _____ Name_____ Date_____	I give permission for access to the internet, including creating websites and using blogs with supervision, on the terms set out above Sign _____ Name_____ Date_____

Appendix 2: Online Safety Incident Management Flow Chart