Woodlane High School

achieving success in a nurturing environment

E-Safety Policy

Updated: May 2025

Next Update: May 2028

Du Cane Road London W12 0TN
Tel: 0208 743 5668 | **Fax:** 0208 743 9138
Headteacher: Claire Maynard | **E-mail:** admin@woodlane.lbhf.sch.uk
Web: www.woodlane.lbhf.sch.uk

1. Introduction to the Policy

The school is aware and acknowledges that increasing numbers of adults and children use technology regularly throughout their daily lives, particularly social networking sites and apps. The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with the safety of our pupils and the reputation of the school. This policy and its associated guidance is also to protect staff and advise school leadership on how to deal with potential inappropriate use of social networking sites. The policy also aims to establish mechanisms to identify, intervene in, and escalate any incident where appropriate. For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

This policy applies to all employees, visitors and pupils of Woodlane High School. This policy does not form part of an employee's contract of employment but acts as clear guidelines and may be amended from time to time, particularly in light of changes in technology.

2. Use of the internet and electronic resources

2.1 Our systems

Woodlane High School provides electronic connectivity for the purpose of education and information retrieval. Ownership of all files and folders on the school's server, shared drives or any database maintained by the school is retained by the school and may not be copied, lent or given to third parties without permission from the Headteacher.

2.2 Security

Efforts to bypass the security of and unauthorised access to the school's systems are strictly prohibited.

2.3 Restrictions on Use

Using the school's equipment and systems, staff and pupils must not:

- Use the IT equipment or systems for unlawful purposes.
- Access or display obscene language or sexually explicit graphics.
- Make copies of copyright-protected materials.
- Use chat rooms, or online gambling.
- Play online games that are inappropriate for the school environment.
- Send or forward material which is illegal, obscene, defamatory, harassing or likely to cause offence. If a member of staff or pupil receive any such material, a member of the senior leadership team should be informed immediately.

- Download new software and applications without confirmation and supervision of the IT Technician or Network Coordinator.
- Share school logins for any services or share WiFi codes.

Within the restrictions above, limited personal use may be made of the Internet, social media and email communications during breaks, within specific areas of the school, such as the Studio and the Playground for pupils. Staff are reminded that they are role models to the pupils and their mobile phone use should reflect this, particularly when using social media. Printers are not for personal use.

2.4 Ownership of specific programmes or databases

Use of some programmes and databases is restricted to certain groups or individuals. Examples include, the 'I Drive' shared management resources, and SIMS. In such cases, the Headteacher must authorise its use by any member of staff.

2.5 IT equipment and support

All employees are responsible for seeking support with queries relating to the general use of our IT equipment and systems by immediately contacting the Network Manager or our external IT support service Turn It On. For non-emergency issues these can be recorded on an online form by the relevant member of staff. The form is checked regularly by Turn It On who can fix problems remotely and record the outcome within the online form. Where further support is required, the technician attends on a Thursday each week. Before attempting to fix a problem, staff should ask the Network Manager to determine if it is something they can or should attempt themselves.

3. Social media

This section of our policy sets out the principles that should be followed when engaging in online communication using "social media" tools. Examples of these tools include Social Networking Sites (e.g. Facebook, LinkedIn), Micro-blogging sites (e.g. Twitter), Blogs, Video and Photo Sharing Websites (e.g. Instagram, YouTube), Forums and Discussion Boards and Online Encyclopedia (e.g. Wikipedia).

3.1 Guiding principles

Woodlane High School values tolerance, respect, equality and diversity. The actions of all staff and pupils should reflect these core principles when they are using social media platforms, particularly due to the public facing role of working with young people and their families.

3.2 Pupils Engaging in Social Media

Social media offer new opportunities to engage in conversations with other individuals and communities with shared interests and we support the desire of our pupils to participate in these online communities as a way of building their social and communication skills. The use of technology can help to increase the confidence of pupils with SEND and provides a range of opportunities to meet, interact and

maintain friendships with others. However, many of these technologies come with associated risks that are increased given the vulnerability of Woodlane pupils. Pupils who are engaging in social media therefore need to ensure that they follow a few guiding principles to protect both themselves and others online. Pupils should also respect the age restrictions and regulations imposed by sites such as Facebook, as these are designed to protect them. The following are extracts from Facebook privacy policy: *"If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us" "We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices."*

3.3 Guidelines for Pupils

- No pupil under 13 should be accessing social networking sites. This is the guidance from both Facebook and Microsoft. There is a mechanism on Facebook where pupils can be reported via the Help screen.
- Pupils should be aware of the possibility that the person they are speaking to is not who they say they are.
- Pupils are not permitted to use mobile phones in school. Phones must be turned off and kept out of sight or handed into the school office for safe keeping. If mobile phones are observed to be being used staff will confiscate the phone and return to the pupil at the end of the day (see mobile phone policy).
- Pupils should not attempt to communicate with members of staff through social networking sites. If pupils attempt to do this, the member of staff is to inform the Headteacher. Parents will also be informed if this happens.
- No school computers are to be used to access social networking sites at any time of day.
- Any attempts to breach security software such as LGfL's firewall will result in a ban from using school ICT equipment.
- Pupils should report anything that they feel uncomfortable with, including; improper contact or cyber bullying to their tutor or a member of the management team immediately.
- Pupils are encouraged to block and delete any contacts who make them feel uncomfortable when online, although in some cases it can be helpful for staff to see copies of messages that are sent, to allow situations to be more easily resolved.
- Pupils should not take pictures / videos or upload images online of themselves or other pupils taken in school.
- Pupils should not take or upload inappropriate images online of themselves or others.
- Woodlane has a zero-tolerance approach to cyber bullying.

3.4 Social Media Guidelines for Staff

The term ‘staff’ may describe the school workforce under the following:

- Those who are directly employed by Woodlane High School (H&F) such as teachers and teaching assistants.
- Those indirectly employed through an agency, such as supply teachers (Vibe etc.) or cleaners (Purgo).
- Those employed by a company/organisation to work directly with the school, such as Speech and Language Therapists, (NHS) or staff delivering SRE work (Image in Action).
- Those who support the school on a voluntary sense, such as the Governing Body or Friends of Woodlane.

School staff are personally responsible for any content which they publish to any form of social media. An employee should always consider carefully before publishing any content online which is relevant to Woodlane High School, and if doing so ensure the views expressed are highlighted as their own, and not the school. However, many topics relating to Woodlane High School are sensitive and should never be discussed, even if the employee is expressing their own opinion. For example, employees must not comment on a pupil, publish any photographs or use names, locations or specific details about an individual online. Nor should staff speculate about specific projects or strategies to be used with those pupils for whom they work closely with. Employees using social media should ensure that their profile and related content is consistent with how both the employee and Woodlane High School would expect the employee to be presented. Careful consideration should be made for any public facing profile and security settings surrounding the account. Employees may not use Woodlane High School to endorse or promote any product, opinion or cause without the prior consent of the Headteacher. Employees are bound by confidentiality and data protection laws. For those employees looking to enhance their knowledge and use of social media, training and guidance can be provided.

3.5 Responsibilities of staff

All staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sexting (also known as youth produced sexual imagery) put children in danger.

- All staff should be aware that safeguarding issues can manifest themselves via peer on peer abuse.
- All staff should be aware of the three areas of risk: Content, Contact & Conduct.
- All staff should be clear as to the school’s policy and procedures with regards to peer on peer abuse.

The DfE document ‘Keeping Children Safe in Education’ is a key document, which outlines many of the risk factors associated with E-Safety. All staff are required to read the document each year and complete a task to demonstrate their

understanding. All new staff, including temporary supply teachers/teaching assistants, cleaning staff, etc. read the document before they begin their first day.

3.6 Content Guidelines

For those staff members who are associated with the school through employment, it is important that staff consider the following:

- Be respectful. When disagreeing with others' opinions, keep it appropriate and polite.
- If you are having an emotional response to something, pause and wait before publishing.
- If you are unsure whether certain content is appropriate to share online, review it carefully or check the content with the management team. If in doubt, don't post it.
- Be accurate. If you make a mistake, update the content and explain what you have done.
- Separate opinion from fact - and make sure that your audience can see the difference.
- Never disclose personal information.

3.7 Official School Use Guidelines

Woodlane does not currently have an official social media channel as part of its wider communications, although news is shared both on the school website, in mail shots to parents and carers and through text. All activity in these official forms are administrated by the management team who are pre-authorised to 'speak' on the school's behalf online. No one should set up or maintain an account on behalf of the school.

4. Teaching Pupils about E-Safety

Woodlane offers E-Safety across the curriculum and endeavours to keep it as a high priority throughout pupils five years at the school. Including:

- The school will undertake regular teaching on the subject of E-Safety and the three areas of risk; Content, Contact and Conduct through both Computing and PSCHE lessons.
- A yearly theme day takes place, exploring the issue in greater detail through art, music, film and other exciting mediums.
- Woodlane employs Turning Point, Respond and Mind, who visit the school to support pupils to explore a range of personal safety and relationship issues. Topics such as photo sharing and cyber-bullying are taught or supported in whole group drama sessions, or 1:1 sessions where the need is greater.
- Displays around the school have been used to raise awareness of E-Safety and provide information in an engaging and accessible way.

- E-Safety is considered a whole school/cross-curricular issue that is supported in each subject. All schemes of work reference the importance of maintaining safety when using technology within that particular subject and the variety of ways that an individual subject can support this.
- All schemes of work covering online safety are age appropriate.
- Parents are made aware of the school's policy regarding E-Safety and in particular, social networking sites. Parents are asked to sign the Woodlane home-school agreement at the start of each year and sign a code of conduct for internet use alongside their child.
- Parents are invited to an annual parent workshop covering E-Safety and the three areas of risk: Content, Contact and Conduct.

5. Cyber Bullying

Cyber Bullying is described as a repetitive act against an individual that causes distress, using technology as the main method of communication. By adopting a firm stance against cyber bullying, Woodlane high School aims to provide a safe and supportive environment for pupils to learn with technology. Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school. This can be a complex area so all cases are investigated fully by the school. This guidance can apply to text, email, mobile phone, app (Whatsapp/Snapchat etc.) social media and any other form of technological cyber bullying. Under certain conditions, the school will be prompted to act under guidance to take the report further. The following are example situations of cyber bullying and the school's responsibility and intended response:

- *"A year 10 child is receiving rude texts from an ex-pupil who left three months ago."* Although this would not specifically be a school responsibility, the school would speak to parents and may contact the new school to broker a resolution.
- *"A child is receiving taunts from peers in the same class. It takes place at weekends using Whatsapp and Facebook."* The school has a duty of care to investigate and work with the families, as they attend the school. The school may report any pupils under 13 to Facebook.
- *"A child is receiving taunts from their year 9 class peers in picture form. It takes place in evenings and at weekends using Snapchat, so the pictures are automatically deleted after a couple of seconds."* The school has a duty of care to investigate and work with the families as they attend the school. However, there is no evidence of the taunts, and there are no restrictions surrounding the use of Snapchat. The school would explain to the parents the serious nature of the allegations, and would encourage greater support from home to monitor the use of Snapchat. School may ask parents to support in the removal of Snapchat from the phones of the victim and alleged perpetrators.
- Once any disclosure is made, the school will hold a thorough investigation and will involve the families. Most cases would be dealt with under the

school's behavior management systems and anti-bullying policy. If parents and carers refuse to engage and bullying continues, it can be referred to the police as harassment.

6. Filtering and monitoring

The school employs a comprehensive strategy to guarantee that it selects websites, applications, and programs that align with the age and proficiency levels of our students. A vigilant oversight is maintained over the school's devices and network, with continuous monitoring and filtering measures in place to ensure a safe and secure digital environment for pupils and staff.

- Staff undergo comprehensive safeguarding training, which includes online safety protocols. They remain vigilant when students use the school's network and devices, ensuring that the filtering and monitoring systems are functioning as intended. Additionally, they provide reports on the activity of pupils' devices to enhance overall safety measures.
- Staff and students are anticipated to promptly report any discovery of unsuitable websites or inappropriate content shared or posted on school network or devices to the designated safeguarding leads or a member of the senior leadership team. Swift action will be taken to remove or block any harmful and inappropriate content by a member of the senior leadership team (Tim Heapy) and the DSL's or the Computing Leader through requests to LGfL for sites to be blocked.
- The school is committed to reporting any online content suspected to be illegal to the relevant authorities, such as the Internet Watch Foundation (IWF) or the Child Exploitation and Online Protection Command (CEOP). Websites considered lawful but unsuitable for Woodlane pupils will be blocked through reporting to LGfL. Parents and guardians will be notified if their child is implicated in any violations of behavior, safeguarding, anti-bullying, and e-safety policies.
- The Computing Leader at the school initiates requests to LGfL for the blocking or unblocking of sites based on staff requests and senior leadership review. They also supervise Meraki to ensure compliance with filtering and monitoring standards for all school mobile devices, such as iPads. Furthermore, the Computing Leader manages the Google Admin account, handling requests for unblocking YouTube videos and facilitating remote access to Google Classroom for pupils. Their responsibilities extend to maintaining the e-safety policy and conducting regular training sessions for staff, students, and parents.
- When students engage in virtual learning from home, the school acknowledges the limited capacity of staff members to control access to inappropriate websites. In such instances, we depend on the collaboration of parents and carers to actively monitor their child's online activities. In cases where students access virtual learning through alternative provisions, such as during respite, we rely on the involved organisations to implement and maintain suitable filtering and monitoring procedures and raise these questions with providers at the outset of a period of online learning.

- The school encourages parents and carers use filtering and monitoring tools at home and offers an annual e-safety workshop for parents to explore this and other e-safety themes including signposting parents and carers to relevant resources. Acknowledging that filtering and monitoring tools alone are insufficient for pupil safeguarding, the school emphasizes the importance of effective classroom management within the school and screen time management at home. Regular education on e-safety and responsible use is deemed crucial to ensure the safety of pupils.
- The school has complied with the DfE's 'filtering and monitoring standards' by designating specific roles and responsibilities for overseeing filtering and monitoring systems. It has regularly reviewed its filtering and monitoring provisions, taking necessary actions to block any harmful or inappropriate content. Additionally, the school has implemented effective monitoring strategies aligned with safeguarding requirements, as detailed in Woodlane's safeguarding and child protection policy.

7. Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to computer systems that can perform tasks typically requiring human intelligence, such as processing natural language, generating content, making predictions, and analysing data. Examples include tools like ChatGPT, image generators, and AI-powered functions in platforms such as Microsoft Office, Canva, and Arbor.

This policy is designed to promote the safe, ethical, and responsible use of AI tools by students, staff, and members of the school community. It aims to ensure AI is used to enhance teaching and learning, while safeguarding against potential misuse. It also supports the development of digital literacy, critical thinking, and awareness of the limitations and risks associated with AI.

The policy complements other key school documents, including the Safeguarding, Data Protection, Acceptable Use, Examinations, and Teaching & Learning policies. It applies to all use of AI technologies on school premises or remotely, whether on school-owned or personal devices. All AI use within the school is subject to regular monitoring to ensure alignment with educational goals, safeguarding principles, and data protection regulations.

The school uses AI responsibly within various educational and administrative applications, including:

- **Arbor** – for pupil information management, data analysis, and summarising key pupil information for external agencies.
- **Canva** – for designing and creating teaching and learning resources.
- **Office 365** – for content generation, document summarisation, and productivity enhancements including drafting pupil reports.
- **Twinkl** – for supporting lesson planning and generating classroom materials.
- **Other applications** – for creating engaging and accessible teaching and learning resources

7.1 Legitimate Use

AI tools may be used in the classroom with teacher supervision, provided they are age-appropriate and align with curriculum aims. Pupils receive guidance on the advantages and risks of AI use through lessons exploring its role in education, business, and wider society.

All AI tools used must be school-approved and comply with data protection and safeguarding requirements. Staff are responsible for reviewing AI-generated content and remain accountable for all materials used or shared.

7.2 Areas of concern

While AI can support learning and productivity, its misuse presents challenges and potential risks. For concerns specific to coursework or examinations, please refer to the school's Examination Policy.

Key areas of concern include:

- **Academic integrity:**
    - Pupils must not use AI to cheat, plagiarise, or produce content dishonestly.
    - Any AI-assisted work must be clearly acknowledged and authorised by teaching staff.
- **Responsible use:**
    - Pupils and staff must avoid excessive dependence on AI tools.
    - Emphasis should remain on critical thinking, independent learning, and creativity.
- **Data protection and privacy:**
    - Uploading personal, sensitive, or identifiable data into AI tools is strictly prohibited.
    - Images of pupils or staff must not be used with AI applications unless explicitly approved for school-authorised projects.

All AI tools used must meet GDPR compliance standards and uphold the privacy of staff and students. Misuse of AI may be treated as a violation of the Acceptable Use or Behaviour Policy. Any breaches or concerns should be reported to the e-safety Lead or the Designated Safeguarding Lead (DSL).

For questions or concerns related to AI and e-safety, please contact the e-safety Lead or DSL.