Holmwood House School Policy for the Appropriate and Safe Use of Technology

Reviewed August 2024
Next Review August 2025

This policy outlines the principles and practices for the safe and appropriate use of technology, including the internet, and artificial intelligence (AI) within our school. It aims to foster a positive and productive learning environment while mitigating potential risks associated with digital technologies.

Opportunities and Risk

The range of opportunities that technology has created extends to a wide range of learning contexts and a greater range of information, resources and content. Using technology appropriately requires pupils to exercise both moral and technical judgement, to think critically, be creative and flexible in their approach to learning. Digital literacy is a capability to which all children have both a right and a need. As with all learning, developing knowledge, skills and understanding in the context of technology is accompanied by a level of risk. This risk is mitigated by the use of appropriate filtering and monitoring software as well as training and teaching which is offered to all stakeholders within the school's community.

Alongside this the school will seek to ensure that risk to pupils is minimised based on the four core principles of

Content- being exposed to inappropriate, harmful or illegal content, for example:pornography, fake news, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation and extremism.

Contact- being subjected to harmful online interaction with other users; for example:peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct- personal behaviour that increases the likelihood of, or causes, harm;for example making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi nudes and/or pornography, sharing other explicit images and online bullying.

Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

Appendices A and B of this document include an extensive list of the different opportunities and risks.

School Strategies

The school strategy will focus on two areas

- Education on Appropriate Use
- Technical and Network Support

There is a wealth of information available to support schools, colleges and parents/carers to keep safe online. A useful list of resources can be found in KCSIE 2024 Appendix B from p163.

Education

a) Curriculum Content

Digital Literacy

Teach students about online safety, cybersecurity, and responsible internet use.

Include modules on data privacy and understanding AI ethics.

Computational Thinking

Introduce coding and programming skills from an early age.

Develop problem-solving skills through computational thinking exercises.

Ethical Use of Technology

Discuss the ethical implications of AI and emerging technologies.Using Internet derived materials in pupils' own work requires at least an understanding that straight copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance.

Promote critical thinking about the role of technology in society.

Research Skills

Judging reasonable material but selecting that which is relevant to their needs, for instance to answer a homework question.

Being critically aware of the materials they read and know how to validate information before accepting its accuracy to question the validity, currency and origins of information – key information handling skills.

b) Staff Education and Professional Development

It is critical that the school puts in place provision to ensure that staff are informed about new tools and best practices in digital education. Staff will also be given time to understand the curriculum and the most effective ways of integrating this into current subjects. This may include internal or external training and support. The general duties of staff are dealt with in further detail in the sections below.

c) Parental Education

The school will ensure that

- Parents have access to the school's policy on the school website and can request a paper copy from the school office.
- Parents will be informed that pupils will be provided with supervised Internet access, and provided with copies of appropriate use agreements
- Parents are engaged through workshops and regular communication about safe technology use at home, guardians about the importance of children being safe online whilst outside of school

Technical Strategies

The school will ensure that its hardware and software systems ensure the following areas are robust and secure

a) **Data Protection;** Ensure all data is encrypted and securely stored. Educate staff and students about the importance of data privacy and GDPR compliance. Only use vetted and approved digital platforms and AI tools that comply with data protection regulations.

b) **Cybersecurity Measures;** Implement robust antivirus and anti-malware software on all school devices; Regularly update software and conduct security audits. Cybersecurity Measures: Ensure all devices and networks are secured with up-to-date antivirus software and firewalls.

c) **Internet Filtering** Use content filtering systems to block inappropriate or harmful websites. Monitor internet usage to ensure compliance with school policies. Content Filtering and Monitoring: Implement robust filtering systems to block access to inappropriate content and monitor internet usage. Filters will need to be managed to ensure that appropriate protocols are in place to safeguard children from potentially harmful and inappropriate material online without unreasonable 'overblocking'. Within this the school may need to consider the requirements and abilities of children of different ages to manage their own use and the need to access information and platforms for educational purposes.

d) **Firewalls** - Filtering and monitoring is carried out by GoGuardian. The filtering allows for devices to be monitored regardless of location (school or at home). Any breaches result in an automated email that is sent to the DSL, the Headteacher and the Head of Phases who then decide what actions need to be taken. The School's firewall/router is **Draytek Vigor 3910** (installed in 2023) which improves the performance, reliability and control of the network. This firewall is responsible for network security, but not monitoring or filtering of websites. As an additional measure, the new firewall uses a special DNS service provided by **Cloudflare** which broadly blocks access to all known adult content and malware websites which applies to all users and devices connected to the school network, even if they are not using GoGuardian.

e) **Domain** - where pupils are using a G-Suite email address to access internet and portals the domain protections and filters will perform an additional safeguard to alert inappropriate searches or attempts to access harmful content.

f) **Devices**

   1) **Mobile Phones** - As part of the above the school plans carefully how to manage the access to 3,4 and 5G on the school premises; pupils bringing a phone to school because they use the school bus or make their own way to and from school, place their phone in the safe storage unit in the front office when they arrive at school in the morning and pick it up at the end of their school day. At this point in time the school recognises that children's access to screen time and the use of smartphones is an ongoing debate. Boarders have supervised use of their phones during a set time period in the evening. Phones are never allowed in the boarding house and dorms.
   2) **Personal Devices** - where schools have one to one schemes that are sourced through the school the devices are set up to run on school based systems. Where pupils are able to bring non-school sourced and personal device in the signature of the device should enable identification on the school system, and the IT manager will ensure that it will not compromise school systems.
   3) **Memory sticks** and other such portable storage devices may be brought into school when specific permission has been given. Before being used on a school device they will be scanned for virus's by the Head of IT or a technician.

Staff Responsibilities

Governance
Will ensure that the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. Reporting Mechanisms: Establish clear procedures for reporting and addressing online safety concerns and incidents. This will include Bellevue Education's Head of Digital Development reviewing standards and discuss with IT staff, the school's DSL and service providers what more needs to be done to support the school in meeting this standard outlined in paragraph 142 of KCSIE September 2024. The effectiveness of the filter and monitoring software is tested as part of governance reviews, and the school testing and monitoring of systems is reviewed at governance.

Responsibilities of the School and Staff
The school will ensure that all staff have undertaken appropriate e-safety training including their applicable roles and responsibilities in relation to online filtering and monitoring. All staff have responsibility to support the appropriate use of technology by pupils. Teachers will encourage and support students in developing good digital habits through

The Online Safety Officer is Oliver White

Role Modelling
- Demonstrate responsible and ethical use of technology.
- Encourage and support students in developing good digital habits.

Supervision and Monitoring
- Actively supervise students' use of technology and the internet.
- Making sure that appropriate monitoring/filtering is taking place, eg GoGuardian or Smoothwall
- Report any concerns or breaches of policy to the designated safeguarding lead.
- **enable skills** in the context of digital literacy, in both using specific platforms and devices and in evaluating the appropriateness, reliability and security of sources and resources

Professional Development
- Participate in training and professional development related to technology and AI in education.
- Stay informed about new tools and best practices in digital education.
- Share ideas and initiatives with colleagues

Curriculum Integration
- Incorporate technology and AI into lesson plans where appropriate ensuring that technology use aligns with educational objectives and enhances learning outcomes
- Pupils are directed to why they are using the technology, how they can access the relevant materials, and what specific sources this might include.

Appendix A - Opportunities for Pupils in Using Technology, the Internet, and Artificial Intelligence

1. **Enhanced Learning Experiences**
   - **Interactive Learning**: Use educational apps, games, and simulations to make learning more engaging and interactive.
   - **Multimedia Resources**: Access videos, podcasts, and virtual tours to complement traditional learning materials.
2. **Access to Information and Resources**
   - **Online Research**: Utilise the internet to access a vast array of information, including scholarly articles, e-books, and databases.

- **E-Libraries**: Use digital libraries and online repositories for research and learning.

3. **Personalised Learning**
- **Adaptive Learning Software**: Employ AI-driven tools that adjust to individual learning paces and styles, providing customised learning paths.
- **Data Analytics**: Use data from educational software to track progress and identify areas where additional support is needed.

4. **Collaboration and Communication**
- **Online Collaboration Tools**: Leverage platforms like Google Classroom and other collaboration tools for group projects and communication.
- **Global Connections**: Connect with peers, experts, and cultures around the world through virtual exchanges and global projects.

5. **Development of Digital Skills**
- **Coding and Programming**: Learn coding languages and develop programming skills through online courses and interactive platforms.
- **Digital Literacy**: Gain proficiency in using various digital tools and platforms, essential for future academic and professional success.

6. **Creative Expression**
- **Digital Art and Design**: Use software for graphic design, video editing, music production, and other forms of digital creation.
- **Content Creation**: Create blogs, podcasts, and videos to express ideas and showcase learning.

7. **Problem-Solving and Critical Thinking**
- **STEM Activities**: Engage in science, technology, engineering, and mathematics (STEM) activities that foster analytical and critical thinking skills.
- **AI Projects**: Participate in projects that involve building and training AI models, enhancing problem-solving abilities.

8. **Career Preparation**
- **Technical Skills**: Develop skills in areas like coding, data analysis, and cybersecurity, which are in high demand in the job market.
- **Exposure to AI and Robotics**: Gain hands-on experience with AI and robotics, preparing for future careers in these fields.

9. **Inclusive Education**
- **Assistive Technologies**: Utilise tools designed to support students with disabilities, such as text-to-speech, speech-to-text, and other accessibility features.
- **Language Support**: Use translation and language learning apps to assist non-native speakers.

10. **Real-World Applications**
- **Simulations and Virtual Labs**: Engage in virtual labs and simulations that provide practical experience without the constraints of physical labs.
- **Project-Based Learning**: Apply knowledge to real-world problems and projects, fostering a deeper understanding of subject matter.

11. **Ethical and Responsible Use of Technology**
- **Digital Citizenship Education**: Learn about the ethical use of technology, including issues like digital footprints, privacy, and the impact of AI on society.
- **Critical Evaluation of Information**: Develop skills to critically assess the credibility and reliability of online information.

12. **Enhanced Assessment and Feedback**
- **Instant Feedback**: Receive immediate feedback on assignments and quizzes through online platforms, enabling timely improvements.
- **E-Portfolios**: Create digital portfolios to track learning progress and showcase achievements over time.

13. **Flexible Learning Opportunities**

- **Remote Learning**: Participate in remote or hybrid learning environments, providing flexibility in how and where students learn.
- **Online Courses and MOOCs**: Enrol in Massive Open Online Courses (MOOCs) and other online classes to explore interests beyond the standard curriculum.

14. **Social and Emotional Learning**

- **Mindfulness Apps**: Use apps that promote mindfulness, mental health, and emotional well-being.
- **Social Platforms for Learning**: Engage in online communities that support learning and provide social interaction, fostering a sense of belonging.

Appendix B - Inappropriate Use of Technology and the Internet - Examples of Inappropriate Use of Technology and the Internet by Pupils

The school is aware that there are ways in which technology and the internet can be used inappropriately. Where pupils misuse technology this will be dealt with through the appropriate policies for Safeguarding and Behaviour, as well as the exclusion policy if necessary.

1. **Seeking to Circumvent Safeguards**
   - The use of Virtual Private Networks (VPNs)
   - The use of SIM driven routers
   - By use of personal email accounts
   - Through using mobile data
2. **Misuse of school email accounts**
   - Using another person's account
   - Sending nuisance or global emails
3. **Cyberbullying**
   - Sending threatening, harassing, or insulting messages to peers through social media, email, or messaging apps.
   - Creating or sharing harmful or embarrassing content about someone else online.
4. **Accessing Inappropriate Content**
   - Visiting websites with violent, explicit, or age-inappropriate material.
   - Downloading or viewing pornography or graphic violence.
5. **Plagiarism and Academic Dishonesty**
   - Copying and pasting content from the internet without proper citation.
   - Using essay mills or other services to purchase academic work.
6. **Unauthorised Access**
   - Hacking into the school's network or other students' accounts.
   - Accessing restricted areas of the school's digital infrastructure without permission
7. **Privacy Violations**
   - Sharing personal information (such as home address, phone number, or personal photos) without consent.
   - Distributing someone else's private information or images without their permission.
8. **Inappropriate Use of Social Media**
   - Posting offensive or inflammatory comments.
   - Participating in or initiating harmful online challenges or trends.
9. **Sexting**
   - Sending or receiving sexually explicit messages, images, or videos.
   - Sharing such content without the consent of the involved parties.

10. **Disruptive Behaviour**
    - Using devices to play games, watch videos, or engage in other non-educational activities during class time.
    - Using social media or messaging apps during lessons, leading to distractions.
11. **Illegal Activities**
    - Downloading or sharing pirated software, music, movies, or other copyrighted material.
    - Engaging in online gambling or other illicit activities.
12. **Misuse of School Resources**
    - Damaging or attempting to damage school technology, such as computers, tablets, or interactive whiteboards.
    - Installing unauthorised software or applications on school devices.
13. **Impersonation**
    - Creating fake profiles or accounts to impersonate others online.
    - Using someone else's login credentials to access their accounts and information.
14. **Spreading Misinformation**
    - Deliberately sharing false or misleading information.
    - Participating in the creation or dissemination of fake news or conspiracy theories.
15. **Unauthorised Recording**
    - Recording teachers or classmates without their knowledge or consent.
    - Sharing or posting recordings taken in school without permission.
16. **Cheating on Assessments**
    - Using digital devices to look up answers during exams or quizzes.
    - Communicating with others to share answers during tests.
17. **Ignoring Digital Etiquette**
    - Using devices in a way that disrupts the learning environment, such as loud notifications or inappropriate ringtones.
    - Failing to respect agreed-upon rules for technology use in the classroom