WREKIN
PREP

E-SAFETY POLICY

2024 - 2025

Last review: September 2024 (Senior Leadership Team)

Date for next review: September 2025

1. E-Safety Policy Statement

Introduction:

The Old Hall School recognises the importance of providing a safe and secure online environment for all members of our school community. As part of our commitment to the well-being and development of our students, staff, and stakeholders, we have developed this E-Safety Policy to ensure responsible and safe use of digital technologies within our educational setting.

Scope:

This policy applies to all individuals associated with The Old Hall School, including students, staff, parents, and any external parties granted access to our digital resources.

Aims and Objectives:

User Responsibility:

Encourage responsible and ethical use of digital technologies.

Promote digital citizenship and awareness of the potential risks associated with online activities.

Education and Awareness:

Provide regular and age-appropriate E-Safety education for students to equip them with the necessary skills to navigate the online world safely.

Offer training and resources for staff to enhance their understanding of E-Safety issues and best practices.

Internet Access:

Ensure that internet access is filtered to restrict access to inappropriate content and to protect users from potential harm.

Monitor online activities to identify and address any breaches of this policy.

Communication and Collaboration:

Foster a culture of open communication regarding E-Safety issues between students, staff, and parents. Encourage collaboration to create a positive online environment.

Reporting and Responding:

Establish clear procedures for reporting any E-Safety concerns or incidents.

Provide support and guidance to individuals affected by E-Safety incidents.

Data Protection:

Implement robust data protection measures to safeguard personal information and sensitive data.

Ensure compliance with relevant data protection legislation.

Roles and Responsibilities:

The Board of Governors: Responsible for reviewing and approving the E-Safety policy and ensuring that sufficient resources are allocated for its implementation.

Principle, Headteacher and Senior Leadership Team: Responsible for overseeing the implementation of the E-Safety policy and providing leadership on E-Safety matters.

Head of Safeguarding (DSL): Appointed to lead the development and implementation of the E-Safety policy, coordinate training, and liaise with relevant stakeholders.

Teachers and Staff: Responsible for incorporating E-Safety education into the curriculum and promoting safe online behaviour.

Students: Expected to adhere to the guidelines outlined in the E-Safety policy and report any concerns promptly.

Parents: Encouraged to actively engage with their child's online activities, participate in E-Safety education, and report any concerns to the school.

Review and Monitoring:

This policy will be regularly reviewed and updated to reflect changes in technology, legislation, and best practices. The effectiveness of the E-Safety measures will be monitored, and adjustments will be made as necessary to ensure a safe online environment for all members of The Old Hall School community.

2. Definitions

E-Safety:

The term "E-Safety" refers to the collective measures and practices in place to ensure the safe and responsible use of digital technologies, including the internet, electronic devices, and online platforms, within the educational environment of The Old Hall School.

Digital Technologies:

"Digital Technologies" encompass all electronic tools, devices, and systems used for communication, collaboration, and information-sharing, including but not limited to computers, laptops, tablets, smartphones, and other internet-enabled devices.

Internet Access:

"Internet Access" refers to the provision of connectivity to the World Wide Web, ensuring that members of The Old Hall School community can access online resources for educational purposes.

Filtering:

"Filtering" involves the use of technological tools to restrict access to inappropriate or harmful content on the internet, ensuring a safe online environment for students, staff, and stakeholders. We conduct filtering through our Senso Cloud monitoring software.

Digital Citizenship:

"Digital Citizenship" encompasses the responsible and ethical use of digital technologies, including awareness of online etiquette, respectful communication, and the understanding of one's rights and responsibilities in the digital world.

Data Protection:

"Data Protection" refers to the practices and policies in place to safeguard personal information and sensitive data, ensuring compliance with relevant data protection legislation, such as the General Data Protection Regulation (GDPR).

E-Safety Education:

"E-Safety Education" involves the provision of structured learning experiences and resources designed to equip students with the knowledge and skills necessary to navigate the online world safely and responsibly.

Digital Literacy:

"Digital Literacy" is the ability to use, understand, and critically evaluate digital technologies, enabling individuals to effectively and safely participate in the digital society.

Online Communication:

"Online Communication" refers to any form of interaction, collaboration, or information exchange that occurs through digital platforms, including email, social media, and other online communication tools.

Incident Reporting:

"Incident Reporting" involves the timely and accurate reporting of any E-Safety concerns or incidents, ensuring that appropriate measures can be taken to address and mitigate potential risks.

Data Breach:

A "Data Breach" is the unauthorised access, disclosure, or loss of sensitive data, requiring immediate attention and remedial action to prevent harm and maintain the security of personal information.

Monitoring:

"Monitoring" involves the systematic observation and oversight of online activities, ensuring compliance with the E-Safety policy and identifying any potential risks or violations.

This definitions section aims to provide clarity and a common understanding of key terms used within The Old Hall School E-Safety Policy.

3. Principles of E-Safety

User Empowerment:

The Old Hall School is committed to empowering all members of the school community, including students, staff, and parents, with the knowledge and skills necessary to use digital technologies safely and responsibly.

Digital Citizenship:

We promote the development of responsible digital citizens who understand the impact of their online actions, respect others in the digital space, and contribute positively to the digital community.

Inclusive Access:

The school ensures inclusive and safe access to digital resources, promoting equality and preventing discrimination in online interactions.

Educational Integration:

E-Safety education is seamlessly integrated into the curriculum to equip students with the awareness and skills required for responsible digital engagement, fostering a culture of lifelong learning.

Collaboration and Communication:

We foster open and effective communication between students, staff, and parents, encouraging collaborative efforts to create a positive and secure online environment.

Risk Assessment and Mitigation:

Regular risk assessments are conducted to identify potential E-Safety risks. Mitigation strategies are implemented promptly to address emerging threats and challenges.

Data Protection and Privacy:

The school is committed to safeguarding personal information and sensitive data, ensuring compliance with data protection legislation and maintaining the highest standards of privacy and security.

Technological Safeguards:

Internet access is filtered to restrict access to inappropriate content, and monitoring mechanisms are in place to detect and address any breaches of the E-Safety policy.

Incident Response and Support:

The school has clear and effective procedures for reporting and responding to E-Safety incidents. Support is provided to individuals affected by such incidents, ensuring their well-being and a swift resolution.

Continual Improvement:

The E-Safety policy is subject to regular review and improvement to adapt to evolving technologies, emerging threats, and changes in best practices, ensuring a proactive and resilient approach to E-Safety.

Community Engagement:

Parents are actively engaged in their child's online activities, and the school collaborates with external stakeholders to promote a shared responsibility for E-Safety within the broader community.

Digital Literacy:

The school promotes digital literacy, enabling students to critically assess and navigate the digital landscape, fostering a generation of individuals who can use technology with confidence and competence.

These principles guide The Old Hall School in creating a safe, supportive, and proactive environment for digital learning, ensuring the responsible and secure use of digital technologies across the school community.

4. Scope and Limitations

Scope:

Applicability:

This E-Safety Policy applies to all individuals associated with The Old Hall School, including students, teaching and non-teaching staff, parents, and any external parties granted access to the school's digital resources.

Educational Setting:

The policy addresses the use of digital technologies within the educational setting of The Old Hall School, including but not limited to classrooms, labs, online platforms, and any other digital environments where learning and school-related activities take place.

Digital Resources:

The policy covers all digital resources provided by the school, including computers, laptops, tablets, smartphones, internet access, software, and online platforms used for educational purposes.

E-Safety Education:

The principles and guidelines outlined in this policy extend to incorporate E-Safety education within the school's curriculum, ensuring that students are equipped with the necessary knowledge and skills to navigate the online world safely.

Communication and Collaboration:

The policy fosters a culture of open communication and collaboration within the school community to create a positive and secure online environment.

Limitations:

Home Environment:

The policy does not extend to the home environment of students. While the school encourages parents to actively engage in their child's online activities, the scope of the policy is limited to school-owned and operated digital resources.

Personal Devices:

The school acknowledges that students may use personal digital devices outside of the school environment. While guidance on responsible use is provided, the school cannot fully control or monitor personal devices.

Third-Party Platforms:

The policy provides guidelines for the use of third-party platforms and online resources directly associated with the school. However, it cannot regulate the policies and practices of external platforms used by individuals outside the school's control.

Unintentional Breaches:

Despite the best efforts and monitoring mechanisms in place, the school acknowledges that unintentional breaches of the E-Safety policy may occur. In such cases, prompt corrective action will be taken to address the situation and prevent reoccurrence.

Evolution of Technology:

The policy is subject to periodic review, but it may not immediately address unforeseen technological advancements or emerging threats. The school is committed to staying abreast of developments to update the policy accordingly.

Legal and Regulatory Changes:

Changes in legislation or regulatory requirements may necessitate updates to the policy. The school will make reasonable efforts to ensure compliance with legal and regulatory frameworks related to E-Safety.

External Stakeholder Actions:

The policy cannot govern the actions of external stakeholders who are not directly affiliated with The Old Hall School. However, efforts will be made to collaborate with external parties to promote a shared commitment to E-Safety.

This Scope and Limitations section provides a clear delineation of the areas covered by The Old Hall School's E-Safety Policy and acknowledges the boundaries and challenges inherent in managing digital safety within an educational context.

5. Responsibilities

Board of Governors:

The Board of Governors holds the ultimate responsibility for approving, reviewing, and endorsing the E-Safety Policy. They ensure that adequate resources are allocated to support the implementation of the policy and provide oversight to guarantee its effectiveness.

Principle Headteacher and Senior Leadership Team:

The Headteacher and the Senior Leadership Team are responsible for the overall implementation of the E-Safety Policy. They provide leadership, promote a culture of E-Safety within the school, and ensure that staff, students, and parents are aware of and adhere to the policy guidelines.

DSL E-Safety Coordinator:

The designated E-Safety Coordinator is appointed to lead the development and implementation of the E-Safety Policy. This individual oversees training programs, coordinates E-Safety initiatives, and serves as the primary point of contact for addressing E-Safety concerns within the school community.

Teachers and Staff:

All teaching and non-teaching staff members share the responsibility of integrating E-Safety education into the curriculum and promoting a safe online environment. They are expected to stay informed about E-Safety best practices, model responsible digital behaviour, and report any E-Safety incidents promptly.

Students:

Students have a responsibility to use digital technologies responsibly and ethically. They are expected to adhere to the guidelines outlined in the E-Safety Policy, actively participate in E-Safety education programs, and report any concerns or incidents they encounter.

Parents:

Parents play a crucial role in supporting E-Safety initiatives. They are encouraged to actively engage in their child's online activities, participate in E-Safety education sessions, and report any concerns or incidents to the school promptly.

Subject Leaders:

Subject leaders, as academic experts in their respective fields, play a vital role in integrating E-Safety education within the curriculum. They are responsible for ensuring that E-Safety principles are embedded in subject-specific lessons, promoting digital literacy, and guiding teachers in fostering a secure online learning environment within their subjects.

Phase Leaders:

Phase leaders, overseeing specific age groups or developmental phases within the school, are integral to the holistic implementation of the E-Safety Policy. They coordinate with subject leaders to ensure a cohesive approach to E-Safety education across phases, addressing age-appropriate concerns and facilitating the development of responsible digital citizens.

IT Committee:

The IT Committee may be formed to provide additional support and expertise in the development and ongoing review of the E-Safety Policy. The committee may include representatives from various stakeholder groups, fostering collaboration and diverse perspectives.

Regular Training and Awareness staff CPD:

The school is committed to providing regular training and awareness programs for all stakeholders, ensuring they are equipped with the knowledge and skills needed to fulfil their responsibilities in promoting a safe online environment.

This Responsibility Section outlines the specific roles and duties of various stakeholders within the Old Hall School, highlighting the collaborative effort required to create a secure and positive digital learning environment.

6. Implementation and Arrangements

Training and Professional Development:

The school is committed to providing regular training sessions and professional development opportunities for all staff members to enhance their understanding of E-Safety issues and equip them with the skills necessary to implement the E-Safety Policy effectively.

Integration into the Curriculum:

E-Safety principles are seamlessly integrated into the curriculum by subject leaders, ensuring that students receive age-appropriate education on responsible digital citizenship across all subjects and developmental phases.

Collaboration with Subject Leaders and Phase Leaders:

Subject leaders and phase leaders collaborate closely with teachers to facilitate the integration of E-Safety into subject-specific lessons and developmental phase activities. They provide guidance and support to ensure a consistent and comprehensive approach.

Monitoring Systems:

The IT department implements and maintains robust monitoring systems to track online activities within the school's digital environment. This includes regular checks on internet filtering, monitoring tools, and other technological safeguards to identify and address potential E-Safety risks.

Incident Reporting and Response:

Clear procedures for reporting E-Safety incidents are communicated to all stakeholders. The school has established response protocols to address incidents promptly, providing support to those affected and taking appropriate measures to prevent reoccurrence.

Internet Filtering and Blocking:

The school employs internet filtering systems to restrict access to inappropriate content, ensuring a safe online environment for students. Regular reviews and updates to filtering policies are conducted to adapt to emerging risks.

Access Controls:

Access controls are implemented to manage user permissions and restrict access to sensitive data. This includes measures to prevent unauthorised access to digital resources and protect the privacy of personal information.

Data Protection Measures:

The school implements robust data protection measures to safeguard personal information and sensitive data. These measures adhere to relevant data protection legislation, ensuring the secure handling and storage of digital information.

Communication Channels:

Effective communication channels are established to disseminate important E-Safety information to students, staff, and parents. This includes newsletters, workshops, and other means to promote a shared understanding of E-Safety principles.

Collaboration with External Agencies:

The school collaborates with external agencies and organisations to stay informed about the latest E-Safety developments and to access additional resources and expertise. This collaborative approach enhances the school's ability to address evolving E-Safety challenges.

Parental Engagement:

The school actively engages parents in E-Safety initiatives, providing information sessions and resources to support them in guiding their children's online activities responsibly.

This Implementation and Arrangements section outlines the practical steps and measures The Old Hall School has in place to bring the E-Safety Policy to life, emphasising training, integration, monitoring, and collaborative efforts to create a secure digital learning environment.

7. Monitoring and Review

Monitoring:

Senso Cloud Monitoring:

The school utilises Senso Cloud as a monitoring tool to actively oversee and analyse digital activities within the school's network. Senso Cloud provides real-time insights into internet usage, application usage, and potential E-Safety concerns.

Real-Time Alerts:

Senso Cloud is configured to generate real-time alerts for any unusual or concerning online activities, allowing the IT support to promptly investigate and address potential risks. Alerts are customised to align with the school's E-Safety policy guidelines.

Internet Filtering Oversight:

Senso Cloud includes features for monitoring and managing internet filtering policies. The school regularly reviews and adjusts filtering settings to ensure that content restrictions align with the school's commitment to providing a safe online environment.

Application and Device Management:

Senso Cloud assists in the monitoring of applications and devices used within the school's digital environment. This includes tracking the usage of specific software and ensuring that all devices comply with E-Safety guidelines.

User Behaviour Analysis:

The monitoring tools provided by Senso Cloud enable the school to conduct user behaviour analysis. This analysis helps identify patterns, trends, and potential areas of concern, allowing for a proactive approach to E-Safety.

Review:

Periodic Policy Review:

The E-Safety Policy undergoes a comprehensive review at regular intervals, ensuring that it remains current and aligned with the school's objectives. Feedback from stakeholders, developments in technology, and insights from monitoring tools contribute to policy updates.

Incident Analysis:

E-Safety incidents are thoroughly analysed during the review process. This includes an examination of incident reports, response protocols, and the effectiveness of preventive measures. Insights gained from incident analysis contribute to continuous improvement.

Legal and Regulatory Compliance:

The school ensures ongoing compliance with legal and regulatory frameworks related to E-Safety. Any changes in legislation are promptly addressed during the review process to maintain a robust E-Safety framework.

This Monitoring and Review section underscores the importance of leveraging technology, collaboration with IT management services, and continuous feedback to monitor and enhance the effectiveness of The Old Hall School's E-Safety measures.

8. DSL, SLT, Staff and Student Responsibilities

Senior Leadership Team (SLT):

The SLT holds responsibility for the overall governance and strategic direction of the school. In the realm of E-Safety, the SLT's involvement in the review and monitoring processes is paramount. They provide the leadership necessary to ensure that E-Safety remains a priority within the school's agenda.

- Strategic Oversight: The SLT sets the strategic direction for E-Safety initiatives, ensuring they align with the broader educational goals of the institution.

- Resource Allocation: They allocate necessary resources, both in terms of finances and personnel, to support effective E-Safety measures, including investing in monitoring tools and training programs.

- Policy Review: The SLT is instrumental in the periodic review of the E-Safety policy. Their input ensures that the policy remains robust, reflecting the evolving digital landscape and aligning with best practices.

- Monitoring Efficacy: The SLT oversees the efficacy of the monitoring systems, ensuring that they function optimally to track and address potential E-Safety risks.

Designated Safeguarding Lead (DSL):

The DSL is the designated individual responsible for overseeing the safeguarding and welfare of students within the school. In the context of E-Safety, the DSL assumes a pivotal role in ensuring that students are protected online.

- Policy Implementation: The DSL ensures that the E-Safety policy is effectively implemented across the school. They provide guidance to staff and students regarding safe and responsible online practices.

- Incident Response: In the event of E-Safety incidents, the DSL leads the response efforts, ensuring that incidents are appropriately addressed, and necessary support is provided to affected individuals.

- Training and Awareness: The DSL coordinates E-Safety training and awareness programs for staff, students, and parents, emphasising the importance of vigilance and responsible digital citizenship.

- Review and Evaluation: Working closely with the SLT, the DSL actively participates in the review and evaluation of E-Safety measures, providing insights into the practical application of policies and the efficacy of safeguarding practices.

The collaboration between the SLT and DSL is essential for creating a cohesive approach to E-Safety. Their joint efforts ensure that policies are not only well-constructed but effectively implemented and continuously improved upon through regular review and monitoring processes.

Responsibilities of Staff and Students

The effective implementation of The Old Hall School's E-Safety policies relies on the active engagement and commitment of both staff and students. Each group has distinct responsibilities to foster a safe digital learning environment:

Responsibilities of Staff:

Curriculum Integration: Staff members are responsible for seamlessly integrating E-Safety principles into their subject lessons, ensuring that students receive age-appropriate education on responsible digital citizenship.

Monitoring and Reporting: Staff should actively monitor students' online activities during lessons, promptly addressing any deviations from acceptable use. They are also required to report any observed E-Safety concerns or incidents to the designated authorities.

Professional Development: Staff members must actively participate in E-Safety training and professional development sessions, staying informed about evolving threats and best practices. This knowledge is crucial for providing effective guidance to students.

Incident Response: In the event of E-Safety incidents, staff members are responsible for implementing the school's response protocols, offering support to affected students, and participating in the resolution process.

Promoting Positive Behaviour: Staff members play a pivotal role in fostering a positive online culture. They should model responsible digital behaviour, encourage respectful communication, and address any inappropriate online conduct promptly.

Responsibilities of Students:

Responsible Use: Students are expected to use digital technologies responsibly, adhering to the guidelines outlined in the E-Safety policy. This includes using devices for educational purposes and refraining from engaging in activities that may compromise their safety or that of others.

Participation in E-Safety Education: Students are responsible for actively participating in E-Safety education programs. They should engage with curriculum activities, workshops, and awareness programs to enhance their understanding of safe online practices.

Reporting Concerns: Students play a vital role in maintaining a safe digital environment by promptly reporting any E-Safety concerns or incidents they encounter. This includes inappropriate content, online harassment, or any other activities that may pose a risk.

Respect for Others: Students should demonstrate respect for others in the digital space, practising positive online behaviour and refraining from any form of cyberbullying, harassment, or misconduct.

Compliance with Policies: Students are expected to comply with all E-Safety policies, as well as related policies such as the Acceptable Use Policy and the Behavior Policy. Adherence to these policies contributes to a secure and respectful online community.

By embracing these responsibilities, both staff and students contribute to the creation of a positive and secure digital learning environment at The Old Hall School.

The Old Hall School E-Safety Policy General Guidelines

Monitoring Using Senso Cloud:

Regularly monitor online activities through Senso Cloud to gain real-time insights into internet and application usage.

Configure Senso Cloud for real-time alerts to promptly address any unusual or concerning online activities.

Curriculum Focus:

Integrate E-Safety principles into the curriculum, ensuring that students receive age-appropriate education on responsible digital citizenship.

Collaborate with subject leaders to embed E-Safety within subject-specific lessons across all phases.

Use of Digital and Video Images:

Obtain consent for the use of digital and video images of students, ensuring compliance with data protection regulations.

Educate students and staff on responsible image-sharing practices and the potential impact on privacy.

Data Protection:

Implement robust data protection measures, ensuring the secure handling and storage of personal information and sensitive data.

Regularly review and update data protection practices in compliance with relevant legislation.

Communication:

Establish effective communication channels to disseminate important E-Safety information to students, staff, and parents.

Encourage open dialogue and collaboration among stakeholders to foster a shared responsibility for E-Safety.

Unsuitable and Inappropriate Activities:

Clearly define and communicate the expectations regarding suitable and unsuitable online activities within the school environment.

Provide guidance on recognizing and reporting inappropriate online content or activities.

Responding to Incidents of Misuse:

Outline clear procedures for reporting and responding to E-Safety incidents promptly.

Ensure that support is provided to individuals affected by incidents, and corrective measures are taken to prevent reoccurrence.

Web Filtering:

Implement web filtering systems to restrict access to inappropriate content, aligning with the school's commitment to a safe online environment.

Regularly review and adjust web filtering settings to adapt to emerging risks.

Use of Mobile Phones and Technology:

Clearly communicate guidelines for the responsible use of mobile phones and other technology within the school premises.

Address the use of personal devices, emphasising responsible behaviour and adherence to school policies.

Conditions of Use - User Shall Not:

- Share personal login credentials or access codes with others.
- Engage in cyberbullying, harassment, or any form of online misconduct.
- Circumvent web filtering or security measures.
- Download or install unauthorised software or applications on school devices.

Summary

The E-Safety policies at The Old Hall School must be used in conjunction with related documents to ensure a comprehensive and cohesive approach to digital safety. The Safeguarding Policy establishes the broader framework for student well-being, aligning with E-Safety measures to create a secure environment. The Acceptable Use Policy provides guidelines for appropriate technology use, complementing the specific E-Safety guidelines. Behaviour Policy and Disciplinary Policy for Staff offer a foundation for addressing misconduct, including E-Safety violations. The Data Protection Policy ensures the secure handling of digital information, reinforcing E-Safety practices. Integrating these policies ensures a unified and robust approach to E-Safety across various facets of school operations.

These general guidelines provide a framework for promoting responsible and safe digital practices within The Old Hall School, covering various aspects of E-Safety including monitoring, curriculum focus, data protection, communication, and appropriate technology use.