E-Safety Policy

Introduction

At Al Madinah Online Secondary School, we are committed to providing a safe and secure digital learning environment for all students. As an online school, we recognize the importance of e-safety to protect students from the potential risks associated with technology, while also enabling them to benefit from online education. This E-Safety Policy outlines the guidelines and procedures in place to ensure that students, staff, and parents are aware of the risks, responsibilities, and best practices related to online safety.

Aims of the Policy

- To protect students and staff from the risks associated with using digital technology and the internet.

- To promote the responsible, safe, and appropriate use of technology for learning.

- To ensure that all members of the school community are aware of the importance of e-safety.

- To outline procedures for dealing with e-safety incidents and breaches of the policy.

- To establish clear guidelines for the use of digital tools, platforms, and communication.

E-Safety Principles

The following principles guide the e-safety practices at Al Madinah Online Secondary School:

- Safety First: The safety of students and staff is the primary consideration when using digital technology and online platforms.

- Education and Awareness: All members of the school community, including students, staff, and parents, will receive ongoing education and training on e-safety.

- Respect and Responsibility: Students, staff, and parents must respect the rights of others when interacting online, avoiding any actions that could harm others or breach their privacy.

- Monitoring and Reporting: Online activity and interactions will be regularly monitored, and any e-safety concerns should be reported promptly to designated staff.

- Confidentiality and Data Protection: All online interactions and personal data will be handled with the utmost care to protect student privacy and ensure compliance with data protection laws.

Roles and Responsibilities

- Designated E-Safety Officer: The designated e-safety officer is responsible for overseeing the implementation of this policy, monitoring e-safety practices, and ensuring that staff, students, and parents are aware of the rules and expectations.

    o Name:

- o Contact:
- Teachers and Staff: All staff members are responsible for:
    - o Promoting safe online practices during lessons.
    - o Monitoring students' use of online platforms and tools.
    - o Reporting any concerns or incidents of inappropriate or harmful behavior online.
    - o Ensuring that students understand the importance of e-safety.
- Students: Students must:
    - o Use online platforms, tools, and digital resources responsibly and respectfully.
    - o Follow guidelines for safe and appropriate online behavior.
    - o Report any suspicious or harmful online activity to a teacher or the designated e-safety officer.
- Parents: Parents are encouraged to:
    - o Educate their children about online safety and the importance of responsible digital behaviour.
    - o Monitor and guide their children's use of technology outside of school hours.
    - o Support the school in ensuring their child's safe use of online platforms.

Acceptable Use of Technology and Online Platforms

- Online Learning Platforms: Students are expected to use the school's online learning platforms, such as [list platforms], for educational purposes only. Any misuse of these platforms, such as engaging in inappropriate chats or accessing non-educational content, will be subject to consequences.
- Communication: Students and staff must communicate in a respectful manner when using school-provided communication channels (email, messaging platforms, etc.). Bullying, harassment, or inappropriate language will not be tolerated.
- Social Media: Students are prohibited from using social media platforms to share or engage in any activities related to the school community during school hours, unless explicitly authorized for educational purposes.
- Personal Devices: The use of personal devices (e.g., smartphones, tablets) for online learning should be in accordance with school guidelines. Students should not use devices to access non-educational content or engage in harmful online behavior.

Online Safety Education
E-safety education is integral to the curriculum, and students will receive ongoing training on how to stay safe online. This includes:

- Understanding Online Risks: Educating students about the dangers of cyberbullying, inappropriate content, online predators, and phishing scams.

- Privacy and Security: Teaching students how to protect their personal information online and how to set strong privacy settings on social media platforms and other online accounts.

- Digital Footprint: Raising awareness about the long-term impact of online behaviour and the importance of maintaining a positive digital reputation.

- Respecting Others Online: Encouraging students to treat others with respect, to report any incidents of online bullying or harmful behaviour, and to seek help when needed.

Reporting E-Safety Concerns

- Students: If a student encounters any e-safety issue, such as cyberbullying, inappropriate content, or harmful online interactions, they should report it immediately to their teacher, the e-safety officer, or a trusted adult.

- Staff: Teachers and staff members are responsible for reporting any concerns or incidents of inappropriate online behaviour involving students or staff. This includes any concerns about a student's safety, mental health, or well-being in relation to their online activities.

- Parents: Parents should immediately inform the school if they become aware of any e-safety concerns affecting their child or other students, whether online or through digital devices.

Monitoring and Filtering

- Monitoring of Online Activity: The school reserves the right to monitor students' online activity during online lessons and on school-provided platforms to ensure compliance with this policy. This may include monitoring chat messages, video interactions, and other online communications.

- Filtering and Blocking: The school has implemented filtering software to block access to inappropriate or harmful websites, online content, and applications. This software is designed to create a safe online environment but does not replace the need for vigilant monitoring by staff and parents.

Dealing with E-Safety Incidents
The school will respond to e-safety incidents following a clear procedure:

- Investigation: Any reports of e-safety incidents will be investigated promptly by the designated e-safety officer or relevant staff members.

- Action: If an incident involves bullying, harassment, or inappropriate behaviour, appropriate action will be taken, which may include sanctions, counselling, or reporting to external authorities such as law enforcement or child protection services.

- Support: Victims of e-safety incidents will be provided with support, including counselling and guidance on how to handle the situation. The school will also work with parents and external agencies as needed to ensure the well-being of the student.

Data Protection and Privacy
The school is committed to protecting the privacy and security of all students' personal data. All online systems, platforms, and communication tools will comply with data protection

regulations, and personal information will only be shared in accordance with the school's privacy policy.

Conclusion

At Al Madinah Online Secondary School, e-safety is a priority, and we are committed to ensuring that all students have a positive and safe experience in the digital learning environment. By working together, we can minimize the risks associated with online activities while maximizing the opportunities for students to learn, grow, and succeed.