Digital Safety and IT Infrastructure Policy

Document Purpose and Legal Framework

The purpose of this policy is to establish a secure, structured, and compliant digital environment that prioritizes the safety, welfare, and data protection of all students and staff. As digital tools become increasingly central to educational growth, managing the associated risks requires clear governance. This document outlines the technical safeguards and behavioral expectations necessary to maintain institutional integrity and protect the school community from online harm.

Compliance with UAE Child Digital Safety (CDS) Law

In strict adherence to the UAE Cabinet Resolution implementing Federal Decree-Law No. 26 of 2025 on Child Digital Safety, Merryland International School enforces definitive age restrictions for social media access. Children under the age of 15 are legally prohibited from creating, operating, or utilizing personal accounts on any social media platforms. This restriction extends to all interactive features, including posting content, commenting, sharing, or participating in public digital groups. Consequently, the school will never require, encourage, or facilitate the use of social media platforms for any educational or extracurricular activities involving students under this age threshold.

Under the CDS Law, parental consent does not constitute a valid exemption from these legal prohibitions. The school maintains a statutory duty to ensure that all students are protected in full compliance with these regulations, irrespective of whether they are accessing external platforms via the school network or personal data plans.

Stakeholder Roles and Responsibilities

Student Expectations and Conduct

Students must utilize school-provided software, networks, and digital devices exclusively for educational purposes aligned with their curriculum objectives. To maintain a focused learning environment and reduce security vulnerabilities, students are strictly prohibited from bringing or using personal electronic devices on school premises.

Account security is an individual responsibility; students must protect their login credentials and are strictly forbidden from sharing passwords with peers. Furthermore, students must adhere to rigorous standards of digital citizenship, which includes refraining from cyberbullying, harassment, or the unauthorized access and distribution of inappropriate content. Academic integrity must be maintained across all digital mediums, meaning students shall not engage in plagiarism or the unauthorized use of copyrighted materials.

Parent and Guardian Obligations

Parents/ Guardians retain a critical role in enforcing digital safety boundaries outside the school environment. In alignment with national legislation, parents must ensure that children under the age of 15 do not create or operate social media accounts.

To maintain structured and secure communications, parents are required to use only school-approved channels when contacting teachers and administrative staff. By partnering with the school, signing the formal Online Safety Agreement, and reinforcing responsible digital behavior at home, parents help establish a unified defense against online risks.

Staff and Faculty Requirements

All staff and volunteers must maintain clear professional boundaries in the digital sphere. Faculty and staff are strictly prohibited from interacting with current students or parents through personal social media accounts. All professional electronic communications must be conducted using official school email addresses, and staff must not use school emails to register personal accounts.

Staff must apply the highest privacy settings to their personal social media profiles to protect their professional standing. In the classroom, teachers must verify that student internet access during instructional hours is strictly for educational purposes. Faculty members must complete ongoing professional development to stay current with emerging technologies and are required to monitor and report student exposure to online risks, such as cyberbullying or online predators.

IT Department Operational Mandates

The IT Department is responsible for the technical execution, documentation, and maintenance of the school's digital infrastructure. Staff within this department must plan and execute regular system updates, apply critical security patches immediately upon release, and conduct routine testing of the network to identify operational vulnerabilities before they risk system failure.

To ensure data resilience against cyber threats like ransomware, the IT Department manages an automated backup strategy using high-end backup software, conducting daily incremental and weekly full backups. These backups must be vaulted and stored securely offline in an isolated physical location. Furthermore, the IT Department deploys robust web filtering and monitoring tools to block harmful content and audits network logs to identify security anomalies. All third-party learning applications must be formally vetted and approved by the IT Department to ensure compliance.

School Leadership Oversight

School Leadership oversees the broader implementation of this policy, ensuring that the IT Department and instructional staff receive adequate resources to maintain a secure infrastructure. Leadership guarantees that institutional practices remain fully compliant with changing regional regulations and internal policies. In the event of an online safety breach, leadership coordinates with counseling services to provide immediate support and intervention for affected students.

Infrastructure, Network, and Data Security

Access Control and Network Defense

Merryland International School encourages protects its digital ecosystem by enforcing multi-factor authentication (MFA) mechanisms across all critical services and administrative platforms. This mechanism mandates multiple forms of verification before granting access to sensitive institutional data. This security is paired with role-based access control, ensuring that personnel can only access resources necessary for their specific organizational duties.

The perimeter of the network is defended by state-of-the-art firewall systems, specifically the SonicWall NSA4900, which monitors incoming and outgoing traffic to mitigate external threats and prevent unauthorized data exfiltration. The network architecture incorporates identity-based firewalls, granting granular visibility into user browsing activity and allowing customized web filtering policies tailored to different age groups. Additionally, endpoint protection platforms are deployed uniformly to block malware execution across all managed hardware.

System Maintenance, Endpoint Security, and Data Integrity

To preserve network integrity, high-end antivirus software, such as Kaspersky Endpoint Security, is installed, monitored, and updated automatically across all school-managed devices. The school's disaster recovery plan details explicit operational procedures to minimize downtime and preserve data availability during a hardware failure or cyber incident.

Physical security controls match these digital measures; access to critical infrastructure rooms, servers, and networking hardware is restricted via biometric authentication or managed secure access cards to prevent physical tampering.

Third-Party Vendor Management

The school maintains strict procurement policies to vet external vendors and service providers. This screening process ensures that all third-party digital tools, platforms, and cloud services comply with local data protection laws and adhere to the same privacy and security standards enforced within the school.

Digital Incidents, Monitoring, and Reporting

A digital incident is defined as any unauthorized, inappropriate, or illegal utilization of technology by a member of the school community. This classification covers actions such as bypassing web filters, sharing explicit or harmful content, participating in cyberbullying, attempting unauthorized access to school databases, or violating any established behavioral codes in an online context.

The IT Department conducts ongoing, systematic analysis of internet traffic and web filter violations to identify potential risks and behavioral issues early. When a digital incident is detected, the school initiates an immediate

investigation. Technical remediation steps are taken to secure any compromised systems or accounts, and appropriate disciplinary or supportive actions are implemented in accordance with school regulations and UAE digital safety legislation.

To ensure this policy remains aligned with emerging technologies, cybersecurity threats, and regulatory updates from the Abu Dhabi Department of Education and Knowledge (ADEK) and UAE federal authorities, the digital infrastructure and safety protocols will undergo regular analysis. The data protection measures, system maintenance logs, and staff digital development needs will be formally reviewed on an annual basis to identify additional training requirements and technical updates necessary to maintain optimal security standards.