DIGITAL POLICY

Being online is an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of children and young people's online world.

The internet and online technology provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks.
E-safety should a fundamental necessity in safeguarding and child protection measures.

In this policy, we define
social media *to mean:* 'Websites and applications that enable users to create and share content or to participate in social networking.'
the word ***staff*** includes temporary and permanent staff, casual staff, and volunteers during their time working with the school.
the word ***parents*** are used to mean the parents, carers and others with parental responsibility for a pupil at the school.

The purpose of this policy statement is to:

1. Prioritize the safety and welfare of children and young individuals when adults, young people, or children utilize the internet, social media, or mobile devices.
2. provide staff and volunteers with the overarching principles that guide our approach to online safety.
3. ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using our school's network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, guardian and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/guardian
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

1. DIGITAL STRATEGY AND OVERSIGHT

1.1. **Digital Strategy :** The Merryland Digital Strategy is designed to establish a clear framework for integrating technology into our educational environment over the next five years. This strategy outlines our commitment to enhancing student achievement, supporting inclusive education, and ensuring the efficient and effective operation of school administration through the deployment of technology.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

1. **Strategic Direction:** Our strategic direction emphasizes the deployment of technology to achieve the following:

- Enhance teaching and learning experiences, making education more engaging and effective.
- Support the efficient and effective management of school administration.
- Foster a culture of continuous improvement through the use of digital tools and data analytics.

2. **Assistive Technology for Inclusion:** We will assess and integrate assistive technology to ensure that all students, including those with disabilities, can participate fully in the educational process. This includes:

- Evaluating current assistive technologies and identifying gaps.
- Procuring and implementing necessary assistive devices and software.
- Training staff on the use of assistive technology to support inclusive education.

3. **Student Digital Skills and Competencies:** Our goals for student digital skills include:

- Ensuring students are proficient in using digital tools for learning and problem-solving.
- Developing competencies in coding, digital communication, and online collaboration.
- Promoting digital citizenship and responsible use of technology.

4. **Development, Procurement, and Implementation Plans:**

- Develop a phased plan for upgrading digital infrastructure, including high-speed internet, modern hardware, and educational software.
- Establish procurement processes to ensure the acquisition of cost-effective and high-quality digital resources.
- Implement technology in classrooms and administrative offices according to a set timeline, with regular reviews and updates.

5. **Security of Digital Systems:** We will implement robust mechanisms to ensure the security of our digital systems, including:

- Regular security audits and risk assessments.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Deployment of advanced cybersecurity measures to protect data and systems.
- Training staff and students on cybersecurity best practices.

6. **Future-proofing Digital Infrastructure:** To future-proof our digital infrastructure, we will:

- Stay informed about emerging technologies and trends.
- Regularly update and upgrade hardware and software to meet evolving needs.
- Ensure scalability of systems to accommodate growth and new functionalities.

7. **Resources and Investment:** The successful implementation of our digital strategy requires:

- A detailed budget plan outlining necessary investments in technology.
- Identification of funding sources and school budget allocations.
- Allocation of resources for ongoing maintenance and upgrades.

8. **Staff Training Requirements:**

- Provide comprehensive training programs for staff to enhance their digital literacy and proficiency in using educational technology.
- Offer professional development opportunities related to emerging technologies and teaching methodologies.
- Create a support system for staff to troubleshoot and resolve technical issues.

9. **Awareness of Emerging Technologies:** We will increase awareness of emerging technologies by:

- Organizing workshops and seminars on topics like Artificial Intelligence, virtual reality, and other innovative tools.
- Encouraging staff and students to explore and experiment with new technologies.
- Partnering with tech companies and educational organizations to stay updated on the latest advancements.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

This digital strategy will guide our efforts over the next five years, ensuring that we meet our goals and provide our students with the skills and opportunities they need to succeed in a digital world.

1.2. Oversight

The Merryland Digital Wellbeing Committee (MDWC) or Lead will oversee the implementation and ongoing management of the school's digital strategy and associated policies.

1. Development and Implementation of Digital Strategy: The MDWC shall be responsible for:

- Developing the school's digital strategy in alignment with the institution's educational goals.
- Ensuring the strategy is implemented effectively across all areas of the school.

2. Annual Review of Digital Strategy and Implementation: The MDWC will conduct an annual review to monitor and evaluate various aspects of the digital strategy:

- **Monitoring Progress:**
  - Assess progress against student learning goals and the school's development and procurement plans.
- **Technology Evaluation:**
  - Evaluate existing technology, software, and online platforms to ensure they align with the strategy's objectives.
- **Risk Assessments:**
  - Perform regular testing and risk assessments of the school's digital systems and infrastructure to ensure they are secure and effective, including backup recovery systems.
- **Cybersecurity Review:**
  - Review and assess the effectiveness of the school's data protection and cybersecurity measures.
- **Technological Needs Assessment:**

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Gather and analyze feedback from staff, parents, and students to re-evaluate the school's technological needs and adjust procurement and development plans accordingly.

- **Staff Development Needs:**
- Re-evaluate staff digital development needs annually and identify additional training requirements to support their professional growth.

3. Policy Development and Review: The MDWC will:

- Develop, implement, and regularly review other school policies related to digital strategy, ensuring they are up-to-date and aligned with overall school goals.

4. Stakeholder Engagement: To ensure well-informed decision-making, the MDWC will:

- Engage with relevant stakeholders, including the Digital Officer, Head of IT, teachers, parents, and students.
- Hold regular meetings and discussions to gather insights and feedback that inform the committee's decisions and actions.

The Digital Wellbeing Committee at Merryland plays a critical role in ensuring that the school's digital strategy is effectively developed, implemented, and reviewed. Through continuous evaluation and stakeholder engagement, the MDWC aims to create a secure, efficient, and inclusive digital environment that supports the school's educational objectives and the wellbeing of its students and staff.

1.3. Digital Liaison Officer

To ensure effective communication and collaboration with the ADEK on matters related to digital competency, safety, and security, Merryland will appoint a dedicated staff member as the Digital Liaison Officer (DLO).

The Digital Liaison Officer will play a crucial role in facilitating communication between the school and the ADEK to align school practices with national policies and guidelines.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Responsibilities of the Digital Liaison Officer:

1. Communication with ADEK:

- Act as the primary point of contact between Merryland and the ADEK for all matters related to digital competency, safety, and security.
- Ensure timely and accurate communication of updates, requirements, and guidelines from the ADEK to the school administration and staff.

2. Digital Competency:

- Collaborate with the ADEK to stay informed about the latest standards and requirements for digital competency in education.
- Work with school staff to integrate these standards into the curriculum and professional development programs.
- Provide regular updates and reports to the school administration on progress and areas needing improvement.

3. Digital Safety and Security:

- Liaise with the ADEK to understand and implement best practices for digital safety and security within the school.
- Ensure the school's digital safety and security measures meet or exceed ADEK guidelines.
- Conduct regular reviews and risk assessments of the school's digital systems to identify vulnerabilities and recommend necessary improvements.

4. Training and Professional Development:

- Organize and facilitate training sessions for staff and students on digital competency, safety, and security, utilizing resources and support from the ADEK.
- Ensure ongoing professional development opportunities for staff to stay current with emerging technologies and digital safety practices.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

5. Policy Implementation and Compliance:

- Assist in the development and implementation of school policies related to digital competency, safety, and security, ensuring alignment with ADEK directives.
- Monitor compliance with these policies and provide feedback to the school administration and ADEK as required.

6. Reporting and Documentation:

- Maintain thorough documentation of all communications, reports, and assessments related to digital competency, safety, and security.
- Prepare and submit regular reports to the ADEK as required, detailing the school's efforts and achievements in these areas.

The appointment of a Digital Liaison Officer at Merryland underscores our commitment to maintaining high standards of digital competency, safety, and security. By fostering close collaboration with the ADEK, we aim to ensure our students and staff are well-equipped to navigate and thrive in an increasingly digital world.

2. DIGITAL COMPETENCIES

2.1 Student Outcomes:

Objective: To equip students with essential digital competencies that will enable them to effectively and safely navigate the digital world, enhance their learning, and prepare them for future academic and professional environments. The competencies will be tailored to the developmental stages of students from early years through to high school.

Grade-wise Digital Competencies and Expected Outcomes

Early Years (KG1 - KG2)

Competencies:

- Basic familiarity with digital devices (tablets, computers).
- Understanding the concept of the internet and its basic uses.
- Introduction to digital safety (asking for help from an adult).

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Expected Outcomes:

- Students will be able to turn on and off digital devices with assistance.
- Students will recognize and name different types of digital devices.
- Students will understand the importance of seeking adult help when encountering unfamiliar content online.

Lower Primary (Grades 1 - 3)

Competencies:

- Basic computer skills (using a mouse, keyboarding).
- Introduction to educational software and applications.
- Basic understanding of internet safety and digital citizenship (e.g., keeping personal information private).

Expected Outcomes:

- Students will be able to navigate basic computer functions and educational software.
- Students will demonstrate the ability to type simple words and sentences.
- Students will identify safe online behavior and know how to handle inappropriate content by informing a teacher or parent.

Upper Primary (Grades 4 - 6)

Competencies:

- Enhanced computer skills (basic word processing, creating simple presentations).
- Introduction to internet research and digital information evaluation.
- Understanding of ethical use of digital resources (avoiding plagiarism).

Expected Outcomes:

- Students will create simple documents and presentations using word processing and presentation software.
- Students will conduct basic internet research and evaluate the reliability of online sources.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Students will explain the importance of citing sources and avoiding plagiarism.

Lower Secondary (Grades 7 - 9)

Competencies:

- Intermediate computer skills (spreadsheets, more advanced word processing and presentations).
- Introduction to coding and basic programming concepts.
- Digital collaboration tools (using online platforms for group projects).

Expected Outcomes:

- Students will use spreadsheets for data entry and simple analysis.
- Students will create more complex documents and presentations with multimedia elements.
- Students will complete basic coding tasks using appropriate programming languages.
- Students will effectively use digital collaboration tools to work on group projects.

Upper Secondary (Grades 10 - 12)

Competencies:

- Advanced digital literacy (data analysis, multimedia production).
- Proficiency in coding and understanding of more complex programming.
- Digital ethics and cybersecurity awareness.
- Preparation for digital demands in higher education and professional settings.

Expected Outcomes:

- Students will conduct complex data analysis and create detailed reports.
- Students will produce high-quality multimedia projects (videos, websites).
- Students will demonstrate advanced coding skills and develop simple software applications.
- Students will articulate key concepts in digital ethics and cybersecurity, and implement best practices in their digital activities.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Integration into the Curriculum

1. **Curriculum Mapping:**
   - **Early Years to Upper Primary:**
     - Digital literacy activities will be integrated into existing subjects, such as using educational apps during language arts or math sessions.
     - Regular "digital safety" sessions will be conducted to reinforce safe online behaviors.
   - **Lower to Upper Secondary:**
     - Dedicated IT classes will cover advanced digital skills, including coding, data analysis, and multimedia production.
     - Digital tools will be incorporated into project-based learning across various subjects to encourage practical application of digital competencies.
2. **Infrastructure and Resources:**
   - Ensure all classrooms are equipped with necessary digital devices and internet access.
   - Provide assistive technologies to support students with additional learning needs.
   - Maintain a digital resource center with access to educational software, coding platforms, and multimedia tools.
3. **Staff Training:**
   - Regular professional development sessions for teachers on integrating digital competencies into their teaching practices.
   - Training on using and troubleshooting digital tools and ensuring cybersecurity measures are followed in the classroom.
4. **Assessment and Evaluation:**
   - Develop rubrics and assessment tools to measure students' progress in digital competencies.
   - Regular feedback and improvement cycles to ensure the digital competencies framework remains relevant and effective.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

5. **Parental Engagement:**

- Inform parents about the digital competencies framework and provide resources for supporting digital learning at home.
- Organize workshops for parents on digital safety and responsible usage to reinforce these practices outside school hours.

2.2 Staff Training:

To ensure that all staff members are equipped with the knowledge and skills necessary to promote the objectives of the school's digital infrastructure and policies, ensuring student digital learning outcomes, data protection, cybersecurity, and digital safety measures.

1. Training Provision

1.1 Role-Based Training

- **Tailored Training Programs:**
  - Develop and implement training programs tailored to the specific roles and responsibilities of different staff members (e.g., teachers, administrative staff, IT staff).
  - Ensure that training is relevant to the day-to-day functions of staff, enhancing their ability to support students and uphold school policies.

1.2 Regular Training Sessions

- **Initial and Ongoing Training:**
  - Provide initial training for new staff members during their onboarding process.
  - Offer ongoing training sessions throughout the academic year to keep staff updated on the latest digital practices, policies, and technologies.

1.3 Professional Development

- **Continuous Professional Development (CPD):**
  - Encourage staff to participate in external CPD opportunities related to digital education, data protection, and cybersecurity.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Allocate time and resources for staff to attend workshops, webinars, and conferences.

2. Training Topics

2.1 Digital Infrastructure and Policies

- **Understanding Infrastructure:**
  - Provide comprehensive training on the school's digital infrastructure, including hardware, software, network systems, and assistive technologies.
  - Ensure staff understand the school's digital policies and how to implement them effectively.

2.2 Student Digital Learning Outcomes

- **Curriculum Integration:**
  - Train staff on integrating digital competencies and expected student outcomes into their curriculum and teaching practices.
  - Emphasize the importance of digital literacy, critical thinking, and responsible digital citizenship.

2.3 Data Protection

- **Data Handling and Compliance:**
  - Educate staff on data protection laws and school policies regarding the collection, processing, and storage of personal information.
  - Cover best practices for securing student and staff data, including consent procedures and data sharing restrictions.

2.4 Cybersecurity

- **Security Awareness:**
  - Provide training on identifying and mitigating cybersecurity threats such as phishing, malware, and ransomware.
  - Teach staff about secure password practices, multi-factor authentication, and the importance of regular software updates.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

2.5 Digital Safety Measures

- **Online Safety:**
  - Train staff on safeguarding students from online risks, including exposure to inappropriate content, cyberbullying, and online predators.
  - Discuss the use of filtering and monitoring systems to ensure a safe digital environment for students.

3. Implementation and Support

3.1 Training Delivery

- **Delivery Methods:**
  - Utilize a variety of training delivery methods, including in-person workshops, online courses, webinars, and hands-on practice sessions.
  - Provide training materials and resources, such as guides, tutorials, and FAQs, accessible through the school's intranet or ORISON learning management system.

3.2 Support Mechanisms

- **Mentoring and Peer Support:**
  - Establish a mentoring system where experienced staff can support and guide less experienced colleagues in understanding and implementing digital policies.
  - Encourage peer collaboration and knowledge sharing through discussion groups and professional learning communities.

3.3 Evaluation and Feedback

- **Assessing Training Effectiveness:**
  - Regularly evaluate the effectiveness of training programs through feedback surveys, assessments, and performance reviews.
  - Use feedback to improve and adapt training content and delivery methods.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

3.4 Resources Allocation

- **Investment in Training:**
  - Allocate sufficient budget and resources for staff training programs, including external training opportunities and technological tools.
  - Ensure that training sessions are scheduled at convenient times to maximize participation and effectiveness.

3. RESPONSIBLE USAGE AND DIGITAL SAFEGUARDING

3.1 Responsible Usage Policies:

To ensure the responsible and secure use of digital technologies by students, parents, staff, and visitors, promoting a safe, ethical, and productive digital environment within the school community.

1. Students

1.1 Responsible Digital Usage

- Students must use school software, networks, services, and digital devices for educational purposes only.
- Adhere to guidelines on appropriate online behavior, digital citizenship, and respect for intellectual property.

1.2 Personal Devices

- Students are permitted to use personal devices on school premises only for educational activities.
- Use of personal devices during extracurricular activities must be approved by a teacher or school official.

1.3 VPN Restrictions

- Use of VPNs by students is prohibited unless explicitly authorized for specific educational purposes.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

1.4 Academic Honesty

- Students must not engage in plagiarism or unauthorized use of copyrighted materials.
- Adhere to school policies on academic honesty and integrity.

1.5 Data Protection

- Students must protect their login credentials and not share passwords.
- Follow guidelines for sharing data securely and ethically.

2. Parents

2.1 Supporting Responsible Usage

- Parents are encouraged to monitor and guide their children's use of digital devices at home.
- Ensure children understand and adhere to the school's digital usage policies.

2.2 Communication and Collaboration

- Use school-approved channels for communication with teachers and school staff.
- Respect privacy and data protection standards when sharing information online.

2.3 Awareness and Training

- Participate in workshops and training sessions provided by the school on digital safety and responsible usage.

3. Staff

3.1 Professional Digital Usage

- Use school software, networks, services, and devices for professional and educational purposes only.
- Maintain professionalism in all online interactions and communications.

3.2 Personal Social Media

- Staff must use the highest privacy settings for personal social media accounts.
- Avoid using school email addresses to create personal accounts.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Do not engage with students or parents through personal social media accounts.

3.3 Password Management

- Set strong passwords for school accounts and update them regularly.
- Do not share passwords with unauthorized individuals.

3.4 Data Sharing and Protection

- Adhere to school policies on data sharing and protection.
- Ensure secure handling and storage of sensitive information.

4. Visitors

4.1 Digital Access

- Visitors may access the school's network and digital services only with explicit permission.
- Use digital resources in accordance with school policies and guidelines.

4.2 Responsible Behavior

- Follow the school's rules on digital usage and online behavior.
- Respect the privacy and security of the school community's data.

Policy Communication

5.1 Dissemination

- Publish the digital usage policies on the school website and include them in the Parent Handbook.
- Provide age-appropriate versions of the policy to students in lower grades and full versions to parents and staff.

5.2 Training and Awareness

- Conduct training sessions for staff, students, and parents on the digital usage policies.
- Use workshops, seminars, and informational materials to raise awareness about responsible digital behavior and cybersecurity.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Monitoring and Enforcement

6.1 Compliance

- Regularly monitor digital usage and adherence to policies within the school.
- Take appropriate disciplinary action in cases of policy violations.

6.2 Review and Update

- Periodically review and update the digital usage policies to address new challenges and technological developments.
- Solicit feedback from the school community to improve and refine the policies.

3.2 Safeguarding Students:

To ensure the safety and well-being of students in digital environments by implementing proactive measures to protect them from online risks and promote responsible digital citizenship.

1. Online Risks Awareness

1.1 Awareness Program

- Implement an age-appropriate awareness program for all students on the benefits and risks of technology.
- Cover topics such as online privacy, cyberbullying, digital citizenship, and safe online behavior.

1.2 Self-Assessment

- Educate students on how to self-assess online risks and make informed decisions about their digital activities.
- Provide resources and tools for students to evaluate the safety of online interactions and content.

2. Filtering and Monitoring

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

2.1 Filtering Systems

- Deploy appropriate filtering systems to monitor and regulate student internet use on school devices and networks.
- Block access to inappropriate content and websites deemed harmful or unsuitable for students.

2.2 Monitoring

- Conduct regular analysis of students' internet usage and web filter violations to identify potential risks or concerns.
- Monitor online activities to detect signs of cyberbullying, inappropriate behavior, or exposure to harmful content.

3. Support and Intervention

3.1 Identification

- Establish procedures to identify and support students who may be at risk due to their digital habits or experiences.
- Encourage students to report any instances of online harassment, bullying, or other concerning behavior.

3.2 Intervention

- Provide counseling and support services to students who have experienced online risks or cyberbullying.
- Implement interventions to address underlying issues and promote positive online behaviors.

4. Virtual Safeguarding Measures

4.1 Virtual Activities

- Implement mechanisms to safeguard students during virtual activities, such as disabling private chat features or monitoring interactions.
- Ensure online platforms used for virtual learning adhere to strict safety and security standards.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

5. Developmental Purpose

5.1 Educational Relevance

- Ensure that student internet access during school hours is for educational purposes and aligned with curriculum objectives.
- Monitor and regulate students' online activities to maintain focus on learning outcomes.

6. Parental Involvement

6.1 Education and Support

- Provide resources and information to parents on digital safety and ways to support their children's online experiences.
- Encourage open communication between parents, students, and school staff regarding online risks and concerns.

7. Reporting and Response

7.1 Incident Reporting

- Establish clear procedures for students, parents, and staff to report online incidents or safety concerns promptly.
- Ensure confidentiality and sensitivity in handling reports of online risks or incidents.

7.2 Response Protocol

- Develop a comprehensive response protocol to address reported online incidents promptly and effectively.
- Provide support to affected students and implement disciplinary measures as necessary.

8. Training and Awareness

8.1 Staff Training

- Provide training to staff on recognizing and addressing online risks and safeguarding students in digital environments.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Equip staff with the knowledge and resources to promote digital safety and responsible usage among students.

9. Collaboration and Review

9.1 Stakeholder Engagement

- Engage with stakeholders, including parents, students, staff, and community organizations, to promote a collaborative approach to student safeguarding in digital spaces.
- Solicit feedback and input from stakeholders to improve policies and practices related to online safety.

9.2 Policy Review

- Regularly review and update the Safeguarding Students Policy to address emerging online risks and reflect best practices in digital safety.
- Ensure alignment with legal requirements and educational standards regarding student welfare and online safety.

3.3 Digital Incidents:

A digital incident occurs when a member of the school community engages in inappropriate or unauthorized use of digital technology. This includes but is not limited to:

- Breach of responsible usage policies.
- Accessing or sharing inappropriate content.
- Inappropriate behaviors or communications online.
- Cyberbullying or harassment.
- Unauthorized access to school systems or data.
- Any other breach of school regulations in an online setting.

2. Identification and Reporting

2.1 Identification

- Regularly monitor school networks, systems, and devices to identify potential digital incidents.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Use automated tools and manual oversight to detect unusual activities or policy violations.

2.2 Reporting

- Any student, parent, staff member, or visitor who identifies or suspects a digital incident must report it immediately to the designated Digital Wellbeing Committee or Lead.
- Reports can be made through a designated reporting system, via email, or in person.
- Maintain confidentiality of the reporting individual to the extent possible, consistent with the need to investigate and address the reported incident.

3. Response and Intervention

3.1 Initial Assessment

- The Digital Wellbeing Committee or Lead will conduct an initial assessment to determine the nature and severity of the incident.
- Categorize the incident based on its impact on individuals and the school community.

3.2 Immediate Actions

- Take immediate steps to contain the incident and prevent further harm.
- This may include restricting access to certain systems, removing inappropriate content, or isolating affected devices.
- Providing support to the students and/ or staff in line with the relevant policy (e.g., *ADEK Employment Policy*, *ADEK Staff Wellbeing Policy*, *ADEK Student Administrative Affairs Policy*, *ADEK Parent Engagement Policy*, *ADEK Student Behavior Policy*, and the *ADEK Student Protection Policy*).

3.3 Investigation

- Conduct a thorough investigation to understand the root cause and extent of the incident.
- Gather evidence, interview involved parties, and document findings.

3.4 Support and Intervention

- Provide support to affected individuals, including counseling services if needed.

- Implement interventions to address harmful behaviors and support positive digital citizenship.
- Apply appropriate disciplinary measures in line with school policies and relevant laws.
- Inform the involved individuals and their parents/guardians of the outcome and any actions taken.

4. Reporting to Authorities

4.1 Mandatory Reporting

- Where required, report digital incidents to relevant authorities, such as the to ADEK and cooperate with the Abu Dhabi Police for investigations.
- Cooperate fully with external investigations and provide necessary documentation and support.

5. Documentation and Review

5.1 Record Keeping

- Maintain detailed records of all reported digital incidents, including initial reports, investigation details, actions taken, and outcomes.
- Ensure records are signed by the Principal and stored securely for auditing purposes, in line with the ADEK's Records Policy.

5.2 Annual Review

- Conduct an annual review of all recorded digital incidents to identify trends and areas for improvement.
- Update policies and procedures based on lessons learned and evolving digital challenges.

6. Communication

6.1 Policy Awareness

- Communicate the Digital Incidents Policy to all members of the school community through appropriate channels, including the school website, handbooks, and training sessions.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Ensure students, parents, staff, and visitors understand their roles and responsibilities in reporting and responding to digital incidents.

7. Parental Involvement

7.1 Monitoring at Home

- Encourage parents to monitor their children's digital activities at home and promote safe and appropriate online behavior.
- Provide resources and training to parents on digital safety and incident reporting.

4. DIGITAL INFRASTRUCTURE

4.1 Digital Devices:

1.1 BYOD Definition

- **Personal Devices:**
  - BYOD refers to the practice of individuals using their personal devices (e.g., laptops, tablets, smartphones) to access school networks, systems, and resources for educational or professional purposes.

1.2 Applicability

- **Authorized Users:**
  - This policy applies to students, staff, and visitors who wish to connect their personal devices to the Merryland School network or utilize school resources.

2. Eligibility and Registration

2.1 Eligible Devices

- **Approved Devices:**
  - Only devices that meet the minimum security standards and compatibility requirements set by Merryland School are eligible for BYOD access.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

2.2 Registration Process

- **Device Registration:**
  - Individuals must register their personal devices with the school's IT department before accessing the school network or systems.
  - Registration may involve providing device information, agreeing to the terms of use, and installing necessary security software or applications.

3. Security Measures

3.1 Minimum Security Requirements

- **Security Standards:**
  - Personal devices must meet minimum security requirements, including up-to-date antivirus software, encryption settings, and password protection, as specified by Merryland School.

3.2 Network Access Controls

- **Access Permissions:**
  - Merryland International School reserves the right to control access permissions for personal devices, including restricting access to certain networks, resources, or applications.

4. Responsible Usage Guidelines

4.1 Acceptable Use

- **Compliance with Policies:**
  - Users must adhere to all Merryland International School policies and guidelines regarding acceptable use of technology, data security, and digital citizenship.

4.2 Data Protection

- **Data Security:**
  - Users are responsible for safeguarding sensitive information stored or accessed on their personal devices, including school-related data and confidential information.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

5. Network Usage

5.1 Network Etiquette

- **Respectful Behavior:**
  - Users must demonstrate respectful and responsible behavior while accessing the school network, refraining from activities that may disrupt network performance or violate school policies.

5.2 Bandwidth Management

- **Fair Usage:**
  - Merryland International School may implement bandwidth management measures to ensure fair and equitable access to network resources for all users, including those with personal devices.

6. Compliance and Monitoring

6.1 Compliance Verification

- **Periodic Audits:**
  - Merryland reserves the right to conduct periodic audits or inspections of personal devices to verify compliance with the BYOD policy and security standards.

6.2 Incident Reporting

- **Security Breaches:**
  - Users must promptly report any security breaches, loss, or theft of personal devices to the school's IT department and follow established incident reporting procedures.

7. Disconnection and Sanctions

7.1 Non-Compliance

- **Consequences of Violation:**
  - Failure to comply with the BYOD policy or misuse of personal devices may result in sanctions, including revocation of network access privileges and disciplinary action.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

8. Disclaimers and Liability

8.1 Liability Limitation

- **User Responsibility:**
  - Merryland School assumes no liability for any loss, damage, or security breaches related to personal devices used within the school environment. Users acknowledge and accept personal responsibility for the security and usage of their devices.

9. Review and Revision

9.1 Policy Review

- **Periodic Evaluation:**
  - The BYOD Policy shall be reviewed and revised periodically to reflect changes in technology, security threats, and regulatory requirements.
  - Feedback from stakeholders may be solicited to identify areas for improvement and enhancement.

9.2 Policy Communication

- **Awareness Campaigns:**
  - Merryland International school shall communicate the BYOD policy to all relevant stakeholders, including students, staff, and visitors, through official channels such as the school website, handbooks, and orientation sessions.

4.2 Digital Systems for Staff:

- Only authorized staff members with specific roles and responsibilities shall be granted access to digital systems relevant to their duties.
- Access permissions shall be assigned based on staff roles and responsibilities to ensure that users have appropriate levels of access to required resources.
- Staff members shall be required to use unique and secure login credentials, including usernames and passwords, to access digital systems.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Multi-factor authentication (MFA) may be implemented for enhanced security.
- Staff shall adhere to password policies, including regular password updates, complexity requirements, and prohibition of password sharing.
- Staff shall receive training on how to use digital systems effectively and securely, including navigating interfaces, accessing resources, and adhering to security protocols.
- Staff members shall be educated about cybersecurity best practices, data protection measures, and their responsibilities in safeguarding sensitive information.
- Staff shall access and handle data stored in digital systems only for legitimate and authorized purposes related to their roles.
- Staff members shall maintain the confidentiality of sensitive information stored in digital systems and refrain from disclosing or sharing such information without proper authorization.
- Merryland shall implement measures to monitor staff access to digital systems and ensure compliance with access policies and procedures.
- Logs of staff access to digital systems shall be maintained for auditing purposes, including timestamps, accessed resources, and user identities.
- Staff members shall promptly report any suspected security breaches, unauthorized access attempts, or unusual system activities to the designated IT personnel.
- School shall have established protocols for responding to security incidents, including investigation, mitigation, and communication with affected staff members.
- Violation of digital systems access policies may result in disciplinary action, including suspension or revocation of system access privileges.
- Staff members acknowledge and accept personal responsibility for their actions and activities while accessing digital systems provided by the school.
- The Digital Systems Access Policy for Staff shall be reviewed and revised periodically to ensure alignment with evolving technology, security standards, and regulatory requirements.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- The school will ensure relevant staff have access to ADEK-provided digital systems, including Learning Management Systems.

4.3 Distance Learning Readiness:

Objective:

School is prepared to facilitate effective and efficient distance learning experiences for students in emergency situations or exceptional circumstances. It aims to maintain continuity of education and support student learning regardless of physical location.

- This policy applies in emergency situations such as temporary school closures due to unforeseen circumstances, prolonged student absences, or exceptional circumstances requiring remote learning.
- Merryland International School utilizes robust LMS (ORISON) to deliver instructional materials, assignments, assessments, and facilitate communication between teachers and students during distance learning.
- Teachers shall ensure that instructional materials and resources provided during distance learning are accessible to all students, including those with additional learning needs, in accordance with the ADEK's Inclusion Policy.
- School shall establish virtual communication channels, such as video conferencing platforms and messaging applications, to facilitate real-time interaction between teachers, students, and parents during distance learning.
- Teachers shall leverage collaborative tools and platforms to facilitate group projects, discussions, and peer collaboration among students, fostering an interactive learning environment.
- Teachers shall conduct synchronous instruction sessions via live video conferencing to deliver lectures, facilitate discussions, and provide immediate feedback to students during distance learning.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Teachers shall provide asynchronous learning activities, such as pre-recorded lectures, online assignments, and discussion forums, to accommodate students' diverse learning schedules and preferences.
- School shall offer technical support services to assist students, parents, and teachers with troubleshooting technical issues related to digital platforms, connectivity, and software applications during distance learning.
- Teachers shall be available to provide academic support, guidance, and clarification to students through virtual office hours, email communication, or scheduled online consultations during distance learning.
- School shall implement measures to ensure that distance learning resources, instructional materials, and communication platforms are accessible to all students, including those with disabilities, in compliance with accessibility standards.
- School shall address equity concerns by providing access to digital devices, internet connectivity, and necessary resources to students from disadvantaged backgrounds or those facing barriers to remote learning.
- School shall maintain regular communication with parents, providing updates on distance learning schedules, assignments, and student progress, and seeking parental feedback and involvement in the learning process.
- School shall offer informational resources, training sessions, and support materials to help parents support their children's learning at home during distance learning periods.
- School shall solicit feedback from students, parents, and teachers regarding their distance learning experiences, challenges encountered, and suggestions for improvement.
- The Distance Learning Readiness Policy shall be reviewed and updated periodically based on feedback, emerging technologies, best practices, and lessons learned from previous distance learning implementations.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

4.4 Assistive Technology:

- This policy applies to students identified as requiring assistive technology accommodations as part of their Individualized Education Plan (IEP) or Documented Learning Plan (DLP).
- School shall conduct comprehensive assessments to identify the specific learning needs and requirements of students eligible for assistive technology support.
- The school's Student Support Team, in consultation with teachers, parents, and relevant specialists, shall develop individualized plans for students receiving assistive technology accommodations.
- School shall select and procure assistive technology tools and resources tailored to meet the unique needs and preferences of each student, ensuring compatibility with existing systems and instructional materials.
- Assistive technology solutions shall be chosen based on principles of universal design, prioritizing accessibility, usability, and flexibility to accommodate a wide range of learning styles and abilities.
- Students receiving assistive technology accommodations shall receive comprehensive training and support to develop proficiency in utilizing the tools effectively to enhance their learning experience.
- Teachers and support staff responsible for implementing assistive technology accommodations shall undergo specialized training to understand the functionality of the tools and effectively integrate them into instructional practices.
- Assistive technology accommodations shall be seamlessly integrated into the curriculum, ensuring that students with additional learning needs have equitable access to educational content, activities, and assessments.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Teachers shall employ differentiated instructional strategies and materials, leveraging assistive technology tools to tailor learning experiences and support diverse learning preferences and abilities.
- School shall ensure that assistive technology tools and digital resources comply with accessibility standards and guidelines to facilitate equitable access for all students.
- The school's IT department shall provide ongoing technical support and maintenance services to address any issues or concerns related to the functionality and accessibility of assistive technology tools.
- The effectiveness of assistive technology accommodations shall be monitored and evaluated regularly through ongoing assessments, progress monitoring, and feedback from students, parents, and educators.
- Prior to implementing assistive technology accommodations, parental consent shall be obtained, and families shall be informed about the purpose, benefits, and implications of using such tools.

4.5 External Providers and Products:

The External Providers and Products Policy outlines guidelines and procedures for selecting, evaluating, and utilizing external IT service providers and products by Merryland International School. This policy aims to ensure the integrity, security, and compatibility of external technologies with the school's digital infrastructure while prioritizing student safety, data privacy, and educational quality.

1. Third party risk assessment framework for selecting external IT service providers

a. Compatibility with Existing School Systems

- Ensure that the external IT service or product is compatible with the school's current digital infrastructure, software, and hardware to facilitate seamless integration and operation.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

b. Secure Management of Data

- Require vendors to implement robust data management practices, including encryption, access controls, and data storage protocols, to safeguard sensitive information and protect against unauthorized access or data breaches.

c. Compliance with Cybersecurity Standards and Frameworks

- Verify that the vendor adheres to recognized cybersecurity standards and frameworks to mitigate risks and vulnerabilities, ensuring the security and integrity of school data and systems.

d. Security against Cyber Threats

- Assess the vendor's measures for identifying, preventing, and responding to cyber threats, including malware, phishing attacks, and other security risks, to ensure the resilience of school operations and data protection.

e. Service Delivery and Backup/Recovery Provisions

- Evaluate the vendor's service delivery capabilities, including responsiveness, reliability, and support provisions, as well as backup and recovery measures to minimize disruptions and ensure continuity of operations in case of system failures or data loss.

f. Reputation and Financial Stability of the Provider

- Conduct background checks and assess the reputation and financial stability of the vendor to ensure reliability, trustworthiness, and long-term viability of the partnership.

g. Adherence to Data Protection Regulations and Policies

- Require vendors to comply with relevant data protection regulations, including the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data, and adhere to ADEK terms and conditions, copyright policies, and data privacy policies regarding the collection, use, and disclosure of information.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

h. Educational Quality and Age-Appropriateness of Content (where relevant)

- Evaluate the educational quality and age-appropriateness of content provided by the vendor, particularly for learning application providers, to ensure alignment with curriculum objectives and suitability for students' developmental stages.

2. Communication to External Vendors Regarding Legal Compliance

Merryland School is committed to upholding the highest standards of data protection, privacy, and copyright compliance in accordance with Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and ADEK regulations. As part of our commitment to legal and ethical practices, we require all external vendors to adhere to these regulations when collecting, using, and disclosing information.

Key Requirements for External Vendors:

1. **Federal Decree-Law No. (45) of 2021 Compliance:**
   - External vendors must comply with the provisions outlined in the Federal Decree-Law on the Protection of Personal Data, ensuring the lawful and ethical handling of personal information.
2. **ADEK Terms and Conditions:**
   - Vendors are expected to adhere to ADEK terms and conditions regarding the collection, use, and disclosure of information, as specified in relevant policies and guidelines.
3. **Copyright Policy:**
   - Vendors must respect copyright laws and policies when using intellectual property, ensuring that materials are used appropriately and with proper authorization.
4. **Data Privacy Policy:**
   - Compliance with data privacy policies is essential to safeguarding the privacy and confidentiality of information collected or processed by vendors on behalf of Merryland International School.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Communication Requirements:

- Merryland International School will communicate these legal requirements to all external vendors during the procurement process and contract negotiations.
- Vendors will be provided with relevant documentation and guidelines outlining their obligations and responsibilities regarding data protection, privacy, and copyright compliance.
- School expects vendors to acknowledge and agree to comply with these requirements as a condition of engagement or contract renewal.

Compliance Monitoring:

- School will implement monitoring and oversight mechanisms to ensure that vendors adhere to legal and regulatory requirements throughout the duration of their engagement.
- Regular audits and reviews may be conducted to assess vendor compliance and address any instances of non-compliance promptly.

Consequences of Non-Compliance:

- Failure to comply with legal and regulatory requirements may result in termination of the vendor's contract or legal action, depending on the severity and impact of the violation.
- School reserves the right to take appropriate measures to protect the interests of students, staff, and stakeholders in the event of non-compliance by external vendors.

5. Data and Cybersecurity

Purpose:

The Digital Data and Cybersecurity Policy of Merryland International School aims to establish comprehensive guidelines and procedures to safeguard digital assets, protect sensitive information, and ensure the integrity of our digital infrastructure. By outlining best practices and security measures, this policy aims to mitigate cyber threats, promote a secure learning environment, and uphold the confidentiality, integrity, and availability of data within our educational institution.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Secure Digital IT Architecture

Access Control:

At Merryland International School, we prioritize the security of our digital infrastructure. We have implemented multi-factor authentication mechanisms for critical services to enhance security. This requires users to provide multiple forms of verification before accessing sensitive data or systems. Additionally, we enforce role-based access control to ensure that individuals have access only to resources and information necessary for their respective roles within our educational institution.

Network Security:

We employ advanced security measures, including state-of-the-art firewall systems like the SonicWall NSA4700, to monitor network traffic, identify potential threats, and protect against unauthorized access or data breaches. Our network security strategy encompasses firewall protection, intrusion detection, and web filtering policies, all aimed at creating a safer online environment for our students. Endpoint protection platforms are also deployed to detect and prevent malware infections across our school network. Furthermore, our use of identity-based firewalls offers granular visibility into user browsing activity, enabling effective monitoring and control of internet access tailored to the specific needs of Merryland International School.

Endpoint Protection:

To maintain a secure digital environment conducive to effective teaching and learning, Merryland International School ensures that high-end antivirus software, such as Kaspersky Endpoint Security, is installed and regularly updated on all school-managed devices. This proactive approach mitigates the risk of malware infections, safeguarding sensitive data and preserving the integrity of our network infrastructure.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Data Backup and Recovery:

We understand the paramount importance of data resilience at Merryland International School. Therefore, we implement a robust backup strategy using high-end Acronis software, which includes daily incremental backups and weekly full backups. These backups are automatically scheduled and executed to ensure consistent and secure backups of critical school data. Furthermore, to enhance security measures, these backups are vaulted and stored offline in a separate physical location, providing an additional layer of protection against cyber threats such as ransomware.

Moreover, our disaster recovery plan outlines comprehensive procedures and resources to swiftly respond to security incidents, ensuring minimal downtime and maintaining continuity of operations. This proactive approach underscores our commitment to safeguarding the integrity and availability of data within Merryland International School's digital ecosystem.

Data Security

At Merryland International School, we are committed to implementing robust data security measures. This includes the implementation of data classification controls to categorize and secure information based on its sensitivity and importance. Additionally, we utilize data loss prevention tools, access controls, and endpoint monitoring solutions to prevent unauthorized access or disclosure of sensitive data within our institution.

Physical Security

To complement our digital security measures, Merryland International School implements strict access controls, such as biometric authentication or access card systems, to prevent unauthorized entry and protect critical infrastructure from potential breaches.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Regulatory Compliance

We adhere to comprehensive policies, procedures, and technological measures to ensure the lawful and ethical handling of student and staff data at Merryland International School. Regular audits and training initiatives are conducted to uphold privacy and security standards across all aspects of data management, ensuring compliance with relevant regulations.

Monitoring and Logging

Continuous monitoring of data access, usage patterns, and network activities enables Merryland International School to proactively mitigate threats and ensure adherence to regulatory requirements for protecting student and staff information. Detailed logs provide valuable insights for thorough investigations, compliance assessments, and proactive security measures.

Secure Software Development

Merryland International School maintains a secure IT infrastructure through cloud structured patch management processes, scheduling updates, routine scans for updates and timely deployment of patches, to mitigate potential vulnerabilities and ensure the security of our systems.

Cloud Security

In line with our commitment to security, Merryland International School ensures compatibility with existing infrastructure and implements seamless integration processes to optimize collaboration, efficiency, and access to educational resources for our students and staff while maintaining the highest standards of security in the cloud environment.

Collaboration Security

To protect sensitive educational information shared among students and staff, Merryland International School employs end-to-end encryption and strict access controls on

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

communication and collaboration platforms. These measures ensure the privacy and integrity of our data in collaborative environments.

Third-Party Security

Merryland International School monitors and vets third-party vendors through stringent procurement policies and regular reviews of vendor security practices. This ensures that our partners comply with data protection regulations and uphold the same high standards of security and privacy that we maintain within our institution.

Through the implementation of this policy, Merryland International School commits to fostering a secure digital environment conducive to effective teaching and learning, while safeguarding the privacy and security of all stakeholders' information.

5.2 System Maintenance:

Merryland International School is committed to maintaining its digital infrastructure to support the educational mission of the school while ensuring data security and operational efficiency. Regular maintenance and updates are crucial to preventing system failures, protecting against cybersecurity threats, and ensuring the optimal performance of all digital systems.

Key Components:

- All operating systems, security systems, and software must be regularly updated to the latest versions to protect against vulnerabilities and ensure compatibility with existing infrastructure.
- Critical updates and patches must be applied as soon as they are released to mitigate security risks.
- Antivirus and anti-malware software must be installed on all school-managed devices.
- Regular updates and scans must be conducted to detect and remove malicious software.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Automated updates and scans should be enabled where possible to ensure continuous protection.
- Regular testing of digital infrastructure and systems is required to ensure they are in good working condition and to identify potential issues before they become critical.
- Testing should include performance evaluations, security assessments, and functionality checks.
- Automated regular backups of critical data must be established and maintained to ensure data integrity and availability in case of system failures or cyber incidents.
- Backups must be vaulted and stored offline or in secure cloud storage, separate from the school network.
- A robust disaster recovery plan must be developed and tested periodically to minimize downtime in case of a security incident or system failure.
- Regular maintenance checks and servicing of physical hardware, such as servers, networking equipment, and other critical infrastructure, must be performed to ensure their longevity and optimal performance.
- Secure access to physical hardware must be ensured to prevent unauthorized access and tampering.
- Comprehensive monitoring systems must be implemented to detect and respond to security incidents in real-time.
- Detailed logs of system activity must be maintained for auditing and analysis purposes, ensuring compliance with regulatory requirements.

Roles and Responsibilities:

- **IT Department:**
  - Responsible for planning, executing, and documenting all maintenance activities.
  - Ensures that all systems are regularly updated and tested.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Implements and monitors backup and recovery procedures.
- Conducts regular audits and security assessments.

- **School Leadership:**
- Oversees the implementation of the maintenance policy and ensures adequate resources are allocated.
- Ensures compliance with regulatory requirements and internal policies.

- **Staff and Faculty:**
- Adheres to the guidelines and practices outlined in the maintenance policy.
- Reports any issues or concerns related to system performance and security.

5.3 Safe Use of External Learning Applications:

School is committed to providing a secure digital learning environment. The use of external learning applications must be carefully managed to ensure that students' data and privacy are protected, and that these applications are educationally beneficial and age-appropriate.

Key Components:

1. **Application Approval:**
- All external learning applications must be reviewed and approved by the IT department before they are used in the classroom.
- Applications must meet the school's standards for data security, privacy, and educational quality.

2. **Data Protection:**
- External learning applications must comply with the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and the ADEK's terms and conditions, copyright policy, and data privacy policy.
- Applications must have strong data encryption and protection measures in place to safeguard students' personal information.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

3. **Single Sign-On (SSO) Systems:**
   - Where possible, external learning applications should be integrated with the school's single sign-on (SSO) systems to streamline access and enhance security.
   - SSO systems should ensure that students use strong, unique passwords and that their credentials are not shared or reused across multiple platforms.
4. **Age-Appropriateness:**
   - Applications must be suitable for the students' age group and educational level.
   - Content within the applications must be vetted for appropriateness and relevance to the curriculum.
5. **Parental Consent:**
   - Parental consent must be obtained before students use any external learning applications that collect or use personal data.
   - Parents must be informed about the purpose of the application, the type of data collected, and how it will be used and protected.
6. **Teacher Training:**
   - Teachers must receive training on the safe and effective use of external learning applications.
   - Training should cover data privacy, security measures, and the educational benefits of the applications.
7. **Usage Monitoring:**
   - The use of external learning applications must be regularly monitored to ensure compliance with the school's data protection and security policies.
   - Any incidents or breaches related to the use of these applications must be promptly reported and addressed.
8. **Vendor Agreements:**

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Agreements with external application vendors must include clauses that ensure compliance with data protection laws and the ADEK's policies.
- Vendors must agree to adhere to the school's standards for data security, privacy, and content appropriateness.

9. **Regular Reviews:**

- The IT department must conduct regular reviews of all approved external learning applications to ensure they continue to meet the school's standards and are being used effectively.
- Any application found to be non-compliant or no longer suitable must be removed from use immediately.

5.4 Safe Virtual Interaction with Invited Visitors:

To ensure the safety and privacy of students during live virtual interactions with invited visitors, in accordance with Merryland International School's safeguarding policies and relevant legal requirements.

This policy outlines the procedures for conducting live virtual interactions with invited visitors, ensuring that students are protected from potential risks and that parental consent is obtained.

Key Components:

1. **Parental Consent:**

- Parental consent must be obtained prior to any live virtual interaction between students and invited visitors.
- Parents must be informed about the purpose of the interaction, the identity of the visitor, and the platform to be used.

2. **Approval from ADEK:**

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- All live virtual interactions with invited visitors must be approved by the ADEK, in accordance with the ADEK Extracurricular Activities and Events Policy and the ADEK Student Protection Policy.
- Requests for approval must include details of the visitor, the purpose of the interaction, and the security measures in place.

3. **Platform Security:**

- Only secure, school-approved platforms are to be used for live virtual interactions.
- Features such as private chat, screen sharing, and recording must be managed to ensure student safety.

4. **Visitor Vetting:**

- Invited visitors must undergo a vetting process to ensure they meet the school's standards for interacting with students.
- Visitors must be informed of the school's safeguarding policies and agree to adhere to them.

5. **Teacher Presence:**

- A teacher or staff member must be present during all live virtual interactions to monitor and manage the session.
- Teachers are responsible for ensuring that interactions remain appropriate and for addressing any issues that arise.

6. **Age-Appropriate Content:**

- The content and nature of the interaction must be age-appropriate and relevant to the students' educational needs.
- Visitors must tailor their presentations or discussions to suit the students' age group and understanding.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

7. **Privacy and Confidentiality:**
   - Students' privacy must be protected at all times. Personal information should not be shared without explicit consent.
   - Sessions must not be recorded without prior consent from parents, students, and the visitor.
8. **Reporting Concerns:**
   - Any concerns or issues arising from live virtual interactions must be reported immediately to school leadership and the relevant authorities.
   - Procedures must be in place for students to report any discomfort or inappropriate behavior during virtual interactions.

Procedures:

1. **Request and Consent Process:**
   - Teachers must submit a request for a live virtual interaction to school leadership, including details of the visitor and the purpose of the interaction.
   - Upon approval, parents must be informed and consent obtained using a standard consent form.
2. **Preparation and Briefing:**
   - Visitors must be briefed on the school's policies and the expected conduct during the interaction.
   - Teachers must ensure the virtual platform is set up securely and that all safety features are enabled.
3. **Conducting the Session:**
   - The teacher must join the virtual session before the students and monitor the interaction throughout.
   - Any inappropriate behavior or technical issues must be addressed immediately.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

4. **Post-Session Review:**

- After the session, the teacher should review the interaction, gather feedback from students, and report any concerns to school leadership.
- A record of the interaction, including consent forms and any incident reports, should be maintained for auditing purposes.

Roles and Responsibilities:

- **Teachers:**
  - Submit requests for virtual interactions and obtain necessary approvals.
  - Ensure parental consent is obtained and manage the interaction during the session.
- **School Leadership:**
  - Approve requests for virtual interactions and ensure compliance with policies.
  - Oversee the implementation of safety measures and address any reported concerns.
- **Parents:**
  - Provide informed consent for their children's participation in virtual interactions.
  - Discuss any concerns with the school and support the safety measures in place.
- **Invited Visitors:**
  - Adhere to the school's safeguarding policies and conduct themselves appropriately during interactions.
  - Respect the privacy and confidentiality of students.

5.5 Backup and Storage:

To ensure the integrity, availability, and security of Merryland International School's data through effective backup and storage practices, safeguarding critical information against data loss, corruption, and unauthorized access.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

This policy applies to all digital data created, received, maintained, and stored by Merryland School, including academic records, administrative data, and personal information of students, staff, and other stakeholders.

Key Components:

1. **Data Classification:**
   - Data should be classified based on its sensitivity and criticality to school operations.
   - Different classes of data may require different backup frequencies and storage methods.
2. **Backup Frequency:**
   - Daily backups for critical data (e.g., student records, financial data).
   - Weekly backups for non-critical data (e.g., general correspondence).
   - Monthly full backups and incremental backups as needed.
3. **Backup Methods:**
   - Use automated backup systems to ensure consistency and reduce the risk of human error.
   - Store backups in multiple locations, including on-site and off-site storage facilities.
4. **Storage Media:**
   - Use secure and reliable storage media for backups, such as encrypted external hard drives, cloud storage services, or network-attached storage (NAS) devices.
   - Regularly test storage media to ensure data integrity and accessibility.
5. **Data Encryption:**
   - Encrypt all backup data to protect it from unauthorized access during storage and transmission.
   - Use strong encryption standards and keep encryption keys secure.
6. **Access Control:**
   - Restrict access to backup data to authorized personnel only.
   - Implement role-based access controls and regularly review access permissions.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

7. **Data Retention:**
   - Establish data retention schedules based on regulatory requirements and organizational needs.
   - Ensure that obsolete or unnecessary data is securely deleted in accordance with data retention policies.
8. **Recovery Procedures:**
   - Develop and maintain detailed data recovery procedures to ensure quick and efficient restoration of data in the event of data loss or corruption.
   - Regularly test recovery procedures to ensure they are effective and up to date.
9. **Monitoring and Auditing:**
   - Regularly monitor backup processes to ensure they are functioning correctly.
   - Conduct periodic audits of backup and storage practices to identify and address potential issues.
10. **Compliance:**
    - Ensure that backup and storage practices comply with relevant data protection laws, cybersecurity standards, and the school's data privacy policy.
    - Regularly review and update backup and storage policies to reflect changes in regulations and technology.

Procedures:

1. **Backup Scheduling:**
   - Establish and maintain a backup schedule that specifies the frequency and scope of backups for different classes of data.
   - Use automated systems to execute backups according to the schedule.
2. **Data Verification:**

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- After each backup, verify the integrity of the data to ensure it has been accurately and completely captured.
- Address any issues detected during verification promptly.

3. **Storage Management:**
   - Label and organize backup media to facilitate easy identification and retrieval.
   - Store backup media in secure, climate-controlled environments to prevent damage.
4. **Disaster Recovery Planning:**
   - Integrate backup and recovery procedures into the school's disaster recovery plan.
   - Conduct regular drills to ensure staff are familiar with recovery procedures and can execute them effectively.
5. **Documentation:**
   - Maintain comprehensive documentation of backup schedules, procedures, and recovery processes.
   - Document any changes to backup and storage practices to ensure continuity and compliance.

Roles and Responsibilities:

- **IT Department:**
  - Implement and manage backup systems and storage solutions.
  - Monitor backup processes, verify data integrity, and conduct recovery tests.
  - Ensure compliance with relevant data protection laws and standards.
- **School Leadership:**
  - Oversee the development and implementation of backup and storage policies.
  - Allocate resources for backup and storage infrastructure.
- **Staff:**
  - Adhere to backup and storage procedures.
  - Report any issues with data integrity or accessibility to the IT department.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

5.6 Cybersecurity Incidents:

To establish procedures for identifying, responding to, managing, and recovering from cybersecurity incidents at Merryland School. This policy aims to minimize the impact of such incidents on school operations, protect sensitive information, and ensure compliance with relevant laws and regulations.

Key Components:

1. **Incident Definition:**
   - A cybersecurity incident is any event that threatens the confidentiality, integrity, or availability of information systems, networks, or data.
   - Examples include data breaches, malware infections, denial-of-service attacks, unauthorized access, and phishing attacks.
2. **Incident Response Team (IRT):**
   - Establish an IRT responsible for managing cybersecurity incidents.
   - The IRT should include members from the IT department, legal team, communications, and relevant administrative staff.
   - Assign roles and responsibilities within the IRT for incident detection, analysis, containment, eradication, recovery, and reporting.
3. **Incident Detection and Reporting:**
   - Implement systems and tools for continuous monitoring and detection of cybersecurity threats.
   - Encourage staff, students, and third parties to report any suspicious activities or potential incidents immediately.
   - Establish clear reporting channels and procedures for timely communication of incidents to the IRT.
4. **Incident Analysis and Classification:**

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Analyze reported incidents to determine their scope, impact, and severity.
- Classify incidents based on predefined criteria (e.g., critical, high, medium, low) to prioritize response efforts.

5. **Incident Containment and Eradication:**

- Implement containment strategies to prevent the spread of the incident and minimize damage.
- Eradicate the root cause of the incident by removing malware, closing vulnerabilities, and taking other necessary actions.

6. **Incident Recovery:**

- Develop and execute a recovery plan to restore affected systems and data to normal operations.
- Ensure that recovery efforts do not reintroduce vulnerabilities or other security issues.

7. **Post-Incident Activities:**

- Conduct a post-incident review to identify lessons learned and areas for improvement.
- Update incident response procedures, security policies, and training programs based on the findings.

8. **Communication and Reporting:**

- Communicate incident details to affected parties, regulatory bodies, and other stakeholders as required by law and school policy.
- Maintain transparency while protecting sensitive information and preserving evidence for potential investigations.

9. **Training and Awareness:**

- Provide regular training to staff and students on recognizing and responding to cybersecurity threats.
- Promote cybersecurity awareness through campaigns, workshops, and ongoing education.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

10. **Compliance and Legal Considerations:**

- Ensure incident response actions comply with relevant laws, regulations, and school policies.
- Collaborate with legal counsel to address potential legal implications of cybersecurity incidents.

Procedures:

1. **Preparation:**

- Develop and maintain an incident response plan outlining detailed procedures for each phase of incident management.
- Conduct regular incident response drills and simulations to test the effectiveness of the plan.

2. **Detection and Reporting:**

- Utilize security information and event management (SIEM) systems for real-time threat detection and alerting.
- Establish a hotline, email address, or online portal for reporting cybersecurity incidents.

3. **Response and Mitigation:**

- Immediately notify the IRT upon detection or reporting of an incident.
- Follow the incident response plan to contain and mitigate the impact of the incident.

4. **Investigation and Analysis:**

- Collect and preserve evidence related to the incident for further analysis and potential legal action.
- Document the timeline and nature of the incident, including affected systems and data.

5. **Recovery and Restoration:**

- Follow the recovery plan to restore normal operations while ensuring system integrity and security.
- Validate that all affected systems are secure before resuming regular activities.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

6. **Post-Incident Review:**
   - Conduct a thorough review of the incident and response actions.
   - Document lessons learned and update incident response procedures accordingly.
7. **Documentation and Reporting:**
   - Maintain comprehensive records of all incidents, including response actions and outcomes.
   - Report incidents to relevant authorities and stakeholders as required.
8. **Continuous Improvement:**
   - Regularly review and update the incident response plan based on new threats, technologies, and lessons learned.
   - Incorporate feedback from post-incident reviews into training and awareness programs.

Roles and Responsibilities:

- **Incident Response Team (IRT):**
  - Lead the response to cybersecurity incidents and coordinate actions across departments.
  - Ensure timely communication and reporting of incidents.
- **IT Department:**
  - Monitor for cybersecurity threats and manage technical aspects of incident response.
  - Implement and maintain security tools and systems.
- **School Leadership:**
  - Provide oversight and resources for incident response activities.
  - Ensure compliance with legal and regulatory requirements.
- **Staff and Students:**
  - Report any suspected cybersecurity incidents promptly.
  - Adhere to cybersecurity policies and participate in training programs.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

6. Data Protection

6.1 Data Protection Policy:

This policy outlines the principles and procedures for the collection, use, storage, and disposal of personal data to protect individuals' privacy rights.

Key Principles:

1. **Lawfulness, Fairness, and Transparency:**
   - Process personal data lawfully, fairly, and transparently.
   - Ensure individuals are informed about how their data is being used and their rights regarding data protection.
2. **Purpose Limitation:**
   - Collect data for specified, explicit, and legitimate purposes.
   - Do not process data in ways incompatible with those purposes.
3. **Data Minimization:**
   - Ensure that personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. **Accuracy:**
   - Keep personal data accurate and up-to-date.
   - Take reasonable steps to rectify or delete inaccurate data promptly.
5. **Storage Limitation:**
   - Retain personal data only for as long as necessary to fulfill the purposes for which it was collected.
   - Implement appropriate measures for the secure disposal of personal data.
6. **Integrity and Confidentiality:**
   - Protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Implement appropriate technical and organizational measures to ensure data security.

7. **Accountability:**

- Demonstrate compliance with data protection principles.
- Maintain records of data processing activities and ensure responsibilities are clearly assigned.

Procedures:

1. **Data Collection:**

- Collect personal data directly from individuals or from authorized third parties.
- Obtain explicit consent from individuals for data processing where required.
- Provide clear information on the purposes of data collection and individuals' rights.

2. **Data Use:**

- Use personal data only for the purposes for which it was collected.
- Ensure data is processed in a manner that ensures appropriate security and confidentiality.

3. **Data Storage:**

- Store personal data securely, using encryption and access controls where appropriate.
- Implement regular data backups and disaster recovery plans.

4. **Data Access:**

- Restrict access to personal data to authorized personnel only.
- Implement role-based access controls and regularly review access permissions.

5. **Data Sharing:**

- Share personal data with third parties only when necessary and with appropriate safeguards.
- Ensure third parties comply with data protection standards and legal requirements.

6. **Data Subject Rights:**

- Inform individuals of their rights regarding their personal data, including the right to access, rectify, erase, restrict processing, and object to processing.
- Provide mechanisms for individuals to exercise their data protection rights.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

7. **Data Breach Management:**
   - Implement procedures for detecting, reporting, and managing data breaches.
   - Notify affected individuals and relevant authorities promptly in the event of a data breach.
8. **Training and Awareness:**
   - Provide regular training on data protection principles and practices to all staff.
   - Promote data protection awareness through ongoing education and communication.
9. **Compliance and Monitoring:**
   - Conduct regular audits and reviews to ensure compliance with data protection laws and policies.
   - Address non-compliance issues promptly and effectively.

Roles and Responsibilities:

- **Data Protection Officer (DPO):**
  - Oversee the implementation and enforcement of the Data Protection Policy.
  - Act as the point of contact for data protection issues and ensure compliance with legal requirements.
  - Conduct regular audits and assessments of data processing activities.
- **School Leadership:**
  - Support data protection initiatives and ensure adequate resources are allocated.
  - Promote a culture of data protection and compliance within the school.
- **Staff:**
  - Handle personal data in accordance with the Data Protection Policy.
  - Report any data protection concerns or breaches to the DPO immediately.
- **Students and Parents:**
  - Provide accurate and up-to-date personal data as required.
  - Respect the data protection rights of others and follow the school's data protection guidelines.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

By adhering to this Data Protection Policy, Merryland School aims to protect personal data, ensure compliance with legal requirements, and foster trust within the school community.

6.2 Sharing Data with ADEK:

This policy applies to all staff responsible for collecting, processing, and sharing data with the ADEK. This policy outlines the procedures for sharing data with the ADEK to safeguard individuals' privacy rights.

Key Principles:

1. **Lawfulness and Compliance:**
   - Ensure all data sharing with the ADEK is conducted in compliance with relevant laws and regulations, including the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data.
   - Obtain necessary consents or authorizations where required.
2. **Data Minimization:**
   - Share only the minimum amount of data necessary to fulfill the ADEK 's requirements.
   - Avoid sharing excessive or unnecessary personal data.
3. **Accuracy:**
   - Ensure the data shared with the ADEK is accurate and up-to-date.
   - Regularly review and update data to maintain accuracy.
4. **Security and Confidentiality:**
   - Implement appropriate technical and organizational measures to protect data during transmission to the ADEK.
   - Ensure data is encrypted and transmitted through secure channels.
5. **Accountability:**
   - Maintain records of data shared with the ADEK, including the type of data, purpose, and date of sharing.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Assign responsibilities for overseeing and managing data sharing activities.

Procedures:

1. **Data Collection:**
   - Collect data required by the ADEK from students, parents, and staff in accordance with school policies and data protection principles.
   - Inform individuals about the purpose of data collection and the potential sharing with the ADEK.
2. **Data Sharing Authorization:**
   - Obtain explicit consent from individuals for sharing their data with the ADEK, where required.
   - Ensure that consent is documented and stored securely.
3. **Data Preparation:**
   - Prepare data for sharing by ensuring it is accurate, complete, and formatted according to ADEK requirements.
   - Remove or redact any unnecessary or sensitive information not required by the ADEK.
4. **Secure Data Transmission:**
   - Transmit data to the ADEK through secure methods, such as encrypted email or secure file transfer protocols (SFTP).
   - Verify the recipient's identity and ensure the data is sent to the correct contact at the ADEK.
5. **Record Keeping:**
   - Maintain detailed records of data sharing activities, including the date, type of data shared, purpose, and recipient.
   - Store records securely and make them available for audits or inspections.
6. **Monitoring and Compliance:**
   - Regularly review data sharing practices to ensure compliance with this policy and relevant laws.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Conduct periodic audits to verify the accuracy and security of data shared with the ADEK.

Roles and Responsibilities:

- **Data Protection Officer (DPO):**
  - Oversee the implementation and enforcement of the data sharing policy.
  - Ensure compliance with legal requirements and data protection principles.
  - Conduct audits and assessments of data sharing activities.
- **School Leadership:**
  - Support data sharing initiatives and ensure adequate resources are allocated.
  - Promote a culture of data protection and compliance within the school.
- **Staff:**
  - Handle data in accordance with this policy when sharing with the ADEK.
  - Report any data protection concerns or breaches to the DPO immediately.
- **Students and Parents:**
  - Provide accurate and up-to-date personal data as required.
  - Respect the data protection rights of others and follow the school's data protection guidelines.

By adhering to this Data Protection Policy, Merryland School aims to protect personal data, ensure compliance with legal requirements, and foster trust within the school community.

6.3 Data Protection Plan:

To ensure the Data Protection Plan remains up-to-date, effective, and compliant with the latest data protection laws and regulations.

This process applies to all aspects of data protection within Merryland School and involves all staff, students, parents, and external parties who handle or process personal data.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

Annual Review Process:

1. **Planning the Review:**
   - Schedule the annual review of the Data Protection Plan at the beginning of each academic year.
   - Assign the responsibility of leading the review process to the Data Protection Officer (DPO).
2. **Assembling the Review Team:**
   - Form a Data Protection Committee including representatives from school leadership, IT, legal, administrative staff, and teaching staff.
   - Include external advisors if necessary, especially for legal and technical expertise.
3. **Gathering Information:**
   - Collect feedback from staff, students, and parents regarding the current data protection practices.
   - Review the results of the previous year's data protection audits and incident reports.
   - Identify any changes in data protection laws and regulations that need to be incorporated.
4. **Assessing Compliance and Effectiveness:**
   - Conduct a thorough assessment of the current Data Protection Plan to ensure it complies with Federal Decree-Law No. (45) of 2021 and other relevant regulations.
   - Evaluate the effectiveness of existing data protection measures and identify areas for improvement.
   - Check the alignment of the Data Protection Plan with the school's digital strategy and operational needs.
5. **Updating the Data Protection Plan:**
   - Revise the Data Protection Plan to address any compliance gaps, incorporate new legal requirements, and improve data protection measures.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Update procedures for data collection, use, retention, and disposal as necessary.
- Enhance technical and organizational measures to protect personal data against emerging cyber threats.

6. **Communicating Changes:**

- Inform all stakeholders (staff, students, parents, and external parties) about the updates to the Data Protection Plan.
- Provide training sessions and resources to ensure everyone understands the new policies and procedures.
- Update the school's website, Parent Handbook, and other relevant documents with the revised Data Protection Plan.

7. **Implementing Updates:**

- Ensure all changes to the Data Protection Plan are implemented promptly and effectively.
- Monitor the implementation process and address any issues that arise.
- Provide support and resources to staff to help them comply with the new data protection measures.

8. **Monitoring and Continuous Improvement:**

- Regularly monitor data protection practices to ensure ongoing compliance and effectiveness.
- Conduct periodic audits and assessments throughout the year to identify and address any new risks or vulnerabilities.
- Maintain a culture of continuous improvement by encouraging feedback and staying informed about best practices in data protection.

Documentation and Reporting:

- Document all stages of the review process, including findings, decisions, and actions taken.
- Prepare a report summarizing the results of the annual review, including any updates made to the Data Protection Plan.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Submit the report to the school leadership and the Data Protection Committee for approval and record-keeping.

7. DIGITAL COMMUNICATIONS

7.1 Digital Media Policy:

To govern the creation, use, and publication of digital media within Merryland International School, ensuring compliance with legal requirements and safeguarding the privacy and rights of all members of the school community.

This policy applies to all staff, students, parents, and external parties involved in capturing, using, and distributing digital media related to Merryland School.

Policy Provisions:

1. Consent for Digital Media

1.1 **Obtaining Consent:**

- **Photographs and Video Recordings:**
  - Schools shall only take photographs and/or video recordings of students after obtaining written consent from parents. In obtaining consent, schools shall inform parents about the purposes for which the photographs and/or video recordings are being taken.
- **Publishing Digital Content:**
  - Schools shall obtain written consent from parents before publishing digital content involving students. Schools shall clearly specify if the student will be identified by name in the publication when obtaining consent.

1.2 **Withdrawal of Consent:**

- Parents and students may withdraw their consent at any time by notifying the school in writing.
- Upon withdrawal of consent, the school shall cease the use of the digital media in future publications and, where feasible, remove the content from existing publications.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

2. Storage and Security of Digital Media

2.1 **Secure Storage:**

- All digital media files shall be stored securely, with access restricted to authorized personnel only.
- Digital media shall be stored in encrypted files or secure storage systems to prevent unauthorized access and ensure data protection.

2.2 **Retention Period:**

- Digital media files shall be retained only for as long as necessary for their intended purpose and shall be securely deleted or archived thereafter in compliance with the school's data retention policy.

3. Use of Personal Devices and Accounts

3.1 **Personal Devices:**

- Staff and students are not permitted to use personal devices to capture or store digital media related to the school without prior authorization.
- Authorized use of personal devices must comply with the school's data protection and security policies.

3.2 **Personal Accounts:**

- Staff members are prohibited from using personal social media accounts to publish school-related digital media.
- Any digital media captured or created for school purposes must be shared through official school channels and accounts.

4. Digital Media Creation and Publication

4.1 **Creation of Digital Media:**

- Digital media created for school purposes must reflect the school's values and be respectful of all individuals involved.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Care must be taken to ensure that the content is appropriate, accurate, and does not infringe on the rights of any individual.

4.2 **Publication of Digital Media:**

- Digital media content to be published must be approved by the school's media team or designated authority.
- Published content must comply with the school's values, legal requirements, and data protection policies.
- Digital media involving students must be published in a manner that safeguards their privacy and dignity.

5. Monitoring and Enforcement

5.1 **Compliance Monitoring:**

- The school shall regularly monitor compliance with this policy and take appropriate actions to address any violations.
- Instances of non-compliance shall be reported to the school administration and addressed in accordance with the school's disciplinary procedures.

5.2 **Policy Review:**

- This policy shall be reviewed annually to ensure it remains up-to-date with legal requirements and best practices.
- Feedback from staff, students, and parents shall be considered in the review process to improve the policy and its implementation.

6. Communication and Training

6.1 **Policy Communication:**

- This policy shall be communicated to all staff, students, parents, and external parties involved in digital media creation and publication.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- The policy shall be made available on the school's website and included in the Parent Handbook.

6.2 **Training:**

- The school shall provide training sessions for staff and students on the proper use and handling of digital media, emphasizing the importance of consent, data protection, and privacy.

By adhering to this Digital Media Policy, Merryland School aims to create a respectful and legally compliant environment for the creation, use, and publication of digital media, protecting the rights and privacy of all members of the school community.

7.2 Social Media Policy:

To establish guidelines for the appropriate use of social media by staff and students of Merryland School, ensuring alignment with the school's values, safeguarding privacy, and promoting responsible digital citizenship.

This policy applies to all staff members and students who engage in social media activities on behalf of Merryland School or in a manner that may impact the school's reputation.

Policy Provisions:

1. Authorized Use of Social Media

1.1 **Official School Accounts:**

- Only authorized personnel designated by Merryland School administration are permitted to create and manage official social media accounts representing the school.
- These accounts shall adhere to the school's branding guidelines and promote the school's mission and values.

2. Personal Social Media Use

2.1 **General Guidelines:**

- Staff members are allowed to maintain personal social media accounts for private use.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- When using personal accounts, staff members must exercise discretion and ensure that their online behavior reflects positively on Merryland School and complies with this policy.

3. Privacy and Confidentiality

3.1 **Student and Staff Information:**

- Staff members are prohibited from sharing confidential or proprietary information related to Merryland School, its students, staff, or operations on social media.
- Personal information about students or staff shall not be disclosed without proper authorization and in accordance with data protection laws.

4. Content and Language Use

4.1 **Professional Conduct:**

- Staff members shall maintain a professional tone and refrain from using language or posting content that could be deemed offensive, discriminatory, or inappropriate.
- Respectful and courteous communication shall be maintained at all times, reflecting the school's values.

5. Interaction with Students and Parents

5.1 **Boundaries:**

- Staff members shall not accept friend requests or follow current students or former students under the age of 18 on personal social media accounts.
- Direct communication with students and parents shall be conducted through official school channels or platforms designed for educational purposes.

6. Posting School-Related Content

6.1 **Approval Process:**

- Before posting school-related content on personal social media accounts, staff members must ensure that such content aligns with Merryland School's values and does not compromise the school's reputation.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Content that identifies or relates to Merryland School should be approved by the administration or designated authority before publication.

7. Monitoring and Compliance

7.1 **Compliance Monitoring:**

- Merryland School reserves the right to monitor staff members' social media activities to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment, depending on the severity of the infraction.

8. Training and Awareness

8.1 **Staff Training:**

- Merryland School shall provide training sessions for staff members on the appropriate use of social media, emphasizing adherence to this policy and the protection of school and personal reputation.
- New staff members shall receive orientation on this policy as part of their onboarding process.

9. Policy Review

9.1 **Annual Review:**

- This policy shall be reviewed annually to incorporate any updates in social media trends, legal requirements, or school needs.
- Feedback from staff and stakeholders shall be considered during the review process to enhance the effectiveness of the policy.

10. Communication of Policy

10.1 **Policy Awareness:**

- Merryland School shall communicate this policy to all staff members, ensuring their understanding and adherence.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- The policy shall be accessible to staff members through the school's intranet or other appropriate channels.

By following this Social Media Policy, Merryland School aims to maintain a positive online presence, protect the privacy of its community members, and uphold its commitment to professionalism and ethical behavior in the digital sphere.

7.3 Personal Social Media Accounts for Staff:

This policy outlines guidelines for the use of personal social media accounts by staff members of Merryland School, ensuring professionalism, safeguarding privacy, and maintaining the school's reputation.

This policy applies to all staff members of Merryland School who use personal social media accounts.

Policy Provisions:

1. Use of Personal Social Media Accounts

1.1 **Account Creation and Settings:**

- Staff members are allowed to maintain personal social media accounts for private use.
- Accounts should be set to the highest possible privacy settings to protect personal and professional interests.

1.2 **Identification and Association:**

- Staff members should not use school-issued email addresses or official titles in personal social media account profiles or handles, except on professional networking platforms like LinkedIn.

2. Interaction with Students, Parents, and Colleagues

2.1 **Boundaries:**

- Staff members should not accept friend requests or follow current students or former students under the age of 18 on personal social media accounts.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- Direct communication with students and parents should be conducted through official school communication channels or platforms designated for educational purposes.

3. Privacy and Confidentiality

3.1 **Confidentiality:**

- Staff members are prohibited from sharing confidential or proprietary information related to Merryland School, its students, staff, or operations on personal social media accounts.
- Personal information about students or staff shall not be disclosed without proper authorization and in accordance with data protection laws.

4. Content and Language Use

4.1 **Professional Conduct:**

- Staff members shall maintain a professional tone and refrain from using language or posting content that could be deemed offensive, discriminatory, or inappropriate.
- Content shared should reflect positively on Merryland School and uphold its values and mission.

5. Communication with Parents

5.1 **Parent Interaction:**

- Staff members should exercise caution when interacting with parents on personal social media accounts to maintain professional boundaries and avoid conflicts of interest.

6. Posting School-Related Content

6.1 **Approval Process:**

- Before posting school-related content on personal social media accounts, staff members must ensure that such content aligns with Merryland School's values and does not compromise the school's reputation.
- Content that identifies or relates to Merryland School should be approved by the administration or designated authority before publication.

7. Monitoring and Compliance

7.1 **Compliance Monitoring:**

- Merryland School reserves the right to monitor staff members' personal social media activities to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment, depending on the severity of the infraction.

8. Training and Awareness

8.1 **Staff Training:**

- Merryland School shall provide training sessions for staff members on the appropriate use of personal social media accounts, emphasizing adherence to this policy and protecting personal and school reputations.
- New staff members shall receive orientation on this policy as part of their onboarding process.

9. Policy Review

9.1 **Annual Review:**

- This policy shall be reviewed annually to incorporate any updates in social media trends, legal requirements, or school needs.
- Feedback from staff and stakeholders shall be considered during the review process to enhance the effectiveness of the policy.

10. Communication of Policy

10.1 **Policy Awareness:**

- Merryland School shall communicate this policy to all staff members, ensuring their understanding and adherence.
- The policy shall be accessible to staff members through the school's intranet or other appropriate channels.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

By adhering to this Personal Social Media Accounts Policy, staff members of Merryland School contribute to maintaining a positive online presence, protecting personal and professional reputations, and upholding the school's commitment to professionalism and ethical behavior in both offline and online environments.

7.4 Communications via Email:

- **Use of Official Email**: All staff members are required to use their Merryland School-issued email accounts for all official communications related to school matters, including but not limited to communication with students, parents, colleagues, and external stakeholders.
- **Prohibited Use of Personal Email**: The use of personal email addresses (e.g., Gmail, Yahoo) for school-related communications is strictly prohibited. This policy ensures the confidentiality, security, and accountability of all school-related correspondence.
- **Confidentiality**: Staff must exercise caution when communicating sensitive or confidential information via email. It is imperative to ensure that emails containing sensitive information are sent only to authorized recipients.
- **Data Protection**: All staff members are responsible for safeguarding the privacy and integrity of data transmitted via email. This includes not sharing passwords, logging out after use, and reporting any suspicious activity promptly.
- **Professionalism**: All emails sent from Merryland School email accounts should reflect professionalism and adhere to the school's code of conduct. Staff members are reminded to use appropriate language and tone in all email communications.
- **Monitoring**: Merryland School reserves the right to monitor email usage to ensure compliance with this policy and to maintain the security and integrity of its information systems.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

- **Training and Support**: Staff members will receive training on email usage policies and procedures as part of their onboarding process. Ongoing support for email-related queries and issues will be provided by the IT department.
- **Compliance**: Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, depending on the severity of the violation and its impact on the school's operations and reputation.

7.5 School Website:

1. **Content Management**:
   - The website content shall be managed by the designated web administrators appointed by the school administration.
   - Content shall include essential information such as contact details, school services, fees, inspection reports, student achievements (with consent), and other relevant information as per Ministry guidelines.
2. **Accuracy and Currency**:
   - It is the responsibility of web administrators to ensure all information published on the website is accurate, current, and reflects the school's values and policies.
   - Updates and revisions to content shall be made promptly to reflect changes in school policies, programs, or events.
3. **Accessibility**:
   - The website shall be designed and maintained to ensure accessibility for users with disabilities, in compliance with accessibility standards.
   - Alternative formats for important documents and information shall be provided upon request for individuals with specific needs.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

4. **Privacy and Data Security**:
   - Personal information collected through the website shall be handled in accordance with the school's Data Protection Policy and applicable data protection laws.
   - Measures shall be implemented to safeguard the security and confidentiality of user data collected through web forms or other interactive features.
5. **Parent and Community Engagement**:
   - The website shall facilitate effective communication with parents through the publication of newsletters, announcements, and event calendars.
   - Opportunities for feedback and inquiries from parents and community members shall be clearly indicated.
6. **Compliance and Governance**:
   - The website shall comply with all relevant laws, regulations, and Ministry guidelines pertaining to website content, data protection, and online communications.
   - Regular audits and reviews of website content and functionality shall be conducted to ensure compliance and effectiveness.
7. **Design and Navigation**:
   - The website design shall prioritize user-friendly navigation, intuitive layout, and responsive design to ensure optimal viewing experience across various devices.
   - Clear pathways to important information such as admissions procedures, curriculum details, and school policies shall be provided.
8. **Digital Media Usage**:
   - Guidelines for the use of digital media, including photographs and videos of students, shall adhere to the Digital Media Policy of Merryland School.
   - Written consent from parents shall be obtained before publishing any digital media content involving students, specifying the purpose and use of such content.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

9. **Review and Updates**:

- This policy shall be reviewed annually and updated as necessary to reflect changes in technology, regulations, or school practices.
- Amendments to the policy shall be communicated to relevant stakeholders and published on the website.

By adhering to this School Website Policy, Merryland School aims to maintain a transparent, informative, and engaging online presence that supports its educational mission and fosters positive relationships with its community.

This policy will be reviewed every year.

Principal

مدرسة الأرض السعيدة العالمية
Tel.: 02 5519626
P.O.Box: 73340
Abu Dhabi - U.A.E
MERRYLAND INTERNATIONAL SCHOOL L.L.C.

Reviewed on 01 June 2026

Merryland International School is an outstanding, ISO 9001-certified, British Curriculum K-12 school located in Abu Dhabi, U.A.E. providing high quality education to pupils of more than 40 nationalities. Merryland has been a pioneer in education for the last four decades remaining true to its motto 'Changing lives...Nations wide'.

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org

ONLINE SAFETY AGREEMENT

Merryland International school understands the importance of children being able to use the internet for education and personal development. This includes social media platforms, games and apps. We aim to support children and young people in making use of these in our work. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

Parents/guardian: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the class teacher. If you have any questions or concerns please speak to the respective class teacher or school administrative authorities.

This agreement is part of our overarching online safety policy

Young person's agreement

- I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to the parent or teacher.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents and/or teacher and am accompanied by a trusted adult.
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to my parents.
- I understand that these rules are designed to keep me safe and I will follow them,

Signatures: We have discussed this online safety agreement and _____[child's name] agrees to follow the rules set out above.

Parent's signature.....
Date .....

Child's signature.....
Date .....

P. B. 73340, Abu Dhabi, United Arab Emirates. +971 (2) 551 9626 merrylandinternational@gmail.com www.merryland.org