MRC-NECC Digital Security Policy

Ref. NECC-AD/IT/POL/2026/001

Version 1.0

Table of Content

1. Overview

This policy defines the digital governance, cybersecurity, and technology use framework of the Mohammed bin Rashid Center for Special Education – Operated by The New England Center for Children – Abu Dhabi (MRC-NECC). It ensures compliance with the ADEK School Digital Policy (v1.1, September 2024), adapted for the Center's specialized autism education program. This document summarizes multiple NECC internal policies into this public facing document.

2. Purpose & Objectives

- Ensure compliance with ADEK's digital, cybersecurity, and data protection requirements.
- Promote safe and ethical use of digital tools across the organization.
- Establish secure management and use of technology infrastructure.
- Support digital literacy and inclusion aligned with individualized learning plans.
- Integrate digital competencies into teaching and therapeutic programs.
- Safeguard digital data and ensure confidentiality and integrity.
- Define accountability for digital safety and technology use.
- Provide ongoing training to maintain compliance and digital fluency

3. Scope

Applies to all staff, contractors, students (as appropriate), and visitors of the Mohammed bin Rashid Center for Special Education (MRC-NECC) with access to NECC-AD digital systems or data. Adaptations apply to ensure developmental appropriateness and therapeutic relevance for students with ASD.

4. Glossary

MRC-NECC	Mohammed bin Rashid Center for Special Education Operated by The New England Center for Children in Abu Dhabi
NECC-AD	The New England Center for Children in Abu Dhabi

5. Definitions

Therapeutic Technology	Digital tools that support learning, communication, or behavior goals in IEPs.
Digital Safeguarding	Systems and processes that protect vulnerable learners from online harm.
Information Assets	Digital or physical data that hold organizational value

6 Applicable Laws and Regulations

- ADEK School Digital Policy v1.1 (2024)
- Federal Decree Law No. (45) of 2021 – Protection of Personal Data
- Federal Decree Law No. (34) of 2021 – Combatting Rumors and Cybercrimes
- ADHICS Framework (where applicable)
- ADEK Inclusion, Safeguarding, and Student Behavior Policies

7 Responsibilities

1) Executive Director
Approves and enforces this policy.

2) Digital Wellbeing Committee
Oversee the Digital Strategy and annual policy review.

3) IT Department
Implements cybersecurity, access control, and data backup.

4) Staff
Comply with responsible usage and safeguarding protocols.

5) Parents
Support safe digital practices at home.

6) Students
Follow school digital safety guidelines where appropriate.

7 Digital Policy Framework

7.1 Digital Strategy and Oversight
- MRC-NECC has developed a Digital Strategy covering infrastructure, training, and inclusion goals.
- MRC-NECC conducts annual reviews including risk assessments and seeks stakeholder feedback.
- MRC-NECC has designated a Digital Safety Lead to liaise with ADEK.

7.2 Digital Competencies
- MRC-NECC has defined achievable learning outcomes for digital literacy appropriate for the unique student population served by MRC.
- MRC-NECC strives to integrate appropriate technology into individualized and classroom instruction.
- MRC-NECC provides all staff training on cybersecurity and data handling.
- MRC-NECC provides parents with relevant digital security awareness content appropriate for the unique student population.

7.3 Responsible Usage & Safeguarding
- Maintain separate Responsible Usage Policies for staff, students/parents, and visitors.
- Unauthorized VPN use is prohibited, and social media conduct is regulated by policy and consistent process for social posts.
- To avoid plagiarism, AI, and content use are required to comply with applicable copyright laws.
- All digital cybersecurity incidents are recorded and investigated.
- NECC delivers age-appropriate online safety programs.

7.4 Digital Infrastructure
- The IT systems at NECC are secured through multi-factor authentication, firewalls, encryption, EDR, persistent monitoring, continuous penetration testing, and regular updates.
- NECC has implemented data loss prevention, endpoint protection, and cloud posture management.
- NECC maintains and regularly reviews an incident response and recovery plan.

7.5 Data Protection and Privacy
- NECC has established a Data Protection Policy outlining consent, retention, and sharing requirements.
- The Data Protection Plan is reviewed annually to ensure compliance with UAE data laws.
- NECC exercises due diligence in vetting third-party suppliers and requires NDAs (Non-Disclosure Agreements,) and contractual construction with UAE law with vendors handling personal data.

7.6 Digital Communications
- NECC obtains written consent before using or publishing student digital media.
- Rules for staff personal social media accounts have been established, communicated and are enforced.
- NECC prohibits private communication between staff and students via personal channels.
- The school website is maintained with ADEK-compliant website content.

8 Inter-Organizational Coordination
The Digital Safety Lead is responsible for this policy and for coordination with the Global Director of Information Security to ensure compliance with ADEK requirements and congruence with existing NECC policies.

9 Policy Compliance & Review
- Adherence to this policy is mandatory.

- Non-Compliance with this policy shall be may result in corrective action in accordance with ADEK regulations and applicable UAE laws.
- The policy will be reviewed and updated annually or as necessary within shorter intervals to ensure continued compliance with UAE regulations.

10   Final Approval

This policy is approved by the Management and is effective as of **19 February 2026.**

End of Policy