مدرسة الريادة المشرقة
BRIGHT RIDERS SCHOOL

School Digital Policy (AY 2024-26)

Introduction

For students to participate in education, the workforce, and modern life in a meaningful way, they must be able to operate in the digital realm. In order to ensure students' safety and security when using the internet, schools must integrate the development of digital skills into all facets of teaching and learning. This policy lays out the fundamental standards that schools must meet in order to develop and implement a digital strategy, offer instruction and learning on digital safety, and use digital technology securely.

Purpose

This policy is formulated:

- To develop and implement a digital strategy regarding their use of technology, goals related to digital competencies and infrastructure, digital security measures, and required resources, as per ADEK's requirement.
- To ensure that school invests in the development of students' digital skills and competencies to empower them to maximize learning opportunities presented by the use of technology.
- To ensure that school educates students on the responsible and safe access and usage of the online environment and protect students from digital content and interactions that are inappropriate or harmful.
- To ensure that school puts in place systems, mechanisms, and procedures that are safe, balanced, and appropriate to safeguard their digital security.
- To ensure that the school complies with the requirements of the Monitoring and Control Center and the Federal Decree Law No. (45) of 2021 on the Protection of Personal Data in the collection, processing, and storage of personal data.

Definitions

Additional Learning Needs	Individual requirements for additional support, modifications, or accommodations within a school setting on a permanent or temporary basis in response to a specific context. This applies to any support required by students of determination and those who have special educational needs and/ or additional barriers to learning, access, or interaction in that specific context (e.g., dyslexic, hearing or visually impaired, twice exceptional, or gifted and/ or talented). For example, a student with restricted mobility may require lesson accommodations to participate in Physical Education and building accommodations to access facilities but may not require any accommodations in assessments. Equally, a student with hearing impairment may require adaptive and assistive technology to access content in class and may also require physical accommodations (e.g., sit in the front of the class to be able to lip read) to access learning.
Assistive Technology	Any item, piece of equipment, software program, or product system that is used to increase, maintain, or improve the functional capabilities of persons with disabilities (ATIA, n.d.).
Bring Your Own Device (BYOD)	Practice wherein schools allow staff and/ or students to do their work on personally owned digital devices.
Bullying	Repeated physical, social, or verbal aggression exercised by students who feel they are in a position of power against other students who are perceived weaker or powerless, to achieve specific gains or draw attention, in a way that hurts the student physically and/ or emotionally. Bullying can be committed by groups or individuals, in online (cyberbullying) or offline settings. The National Policy for the Prevention of Bullying in Educational Institutions (MoE, n.d.) provides a complete framework for bullying and cyberbullying.
Cyberbullying	Bullying that takes place online. Online bullying can follow the bullied student wherever they go via social networks and mobile phones and has a wider reach than bullying in the real world.
Cybersecurity Incident	A breach that threatens the confidentiality, integrity or availability of an organization's information systems or sensitive data (IBM, n.d.).
Data Protection	The process of safeguarding data from corruption, compromise, unauthorized access, or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable (SNIA, n.d.).

Digital Device	A device used for audio, video, or text communication, or any other type of computer or computer-like instrument, including, but not limited to cell phones, smart watches, tablets, and laptops.

Digital Incident	An instance where a member of the school community engages in the inappropriate use of digital technology. This includes a breach of the reasonable usage policies, the accessing of inappropriate content, inappropriate behaviors or communications, cyberbullying, and/ or any other breach of school regulations in an online setting.
Digital Fluency	The state of being a competent, confident, safe, responsible, creative, and curious user of technology.
Documented Learning Plan	A plan which outlines any personalized learning targets, modifications to curriculum, additional support, or tools for learning which are agreed by school staff, parents, and students (where appropriate), including Individual Educational Plans (IEP), Individual Support Plans (ISP), Individual Learning Plans (ILP), Behavior Support Plans (BSP), Advanced Learning Plans (ALP), etc. This may be to address any specific identified academic, behavioral, language, or social and emotional need.
Parent	The person legally liable for a child or entrusted with their care, defined as the custodian of the child as per the Federal Decree Law No. 3 of 2016 Concerning Child Rights.
Personal Information	Information relating to individuals who are identifiable directly from the information in question, or who can be indirectly identified from that information in combination with other information.
Risk Assessment	A systematic process of evaluating the potential risks that may be involved in an activity or undertaking.
Safeguarding	Protecting students from the risks of harm, including maltreatment and other types of risks that impact their overall health and development, wellbeing, and safety.
SaaS Security Posture Management (SSPM)	A type of automated security tool for monitoring security risks in software-as-a-service (Saa S) applications. It also identifies misconfigurations, unnecessary user accounts, excessive user permissions, compliance risks, and other cloud security issues.
Social Media	A means of social interaction in which people create, share, and/ or exchange information and ideas in virtual communities and networks, including, but not limited to, platforms such as Facebook, Twitter, Instagram, LinkedIn, and YouTube (Tufts University, n.d.).

Visitor	For the purpose of this policy, a visitor is any temporary visitor (e.g., a parent or a relative of a student, prospective student and their parents, inspectors, contractors, etc.) entering the school premises. An invited visitor is anyone visiting the school on a temporary basis to interact with students (i.e., a speaker, career fair representative, etc.) and includes volunteers, who are engaged by an educational institution on a non-remunerated basis to interact with students (e.g., parent chaperones, etc.).

Policy

1. Required Documentation

1.1 Bright Riders School has formally developed and implemented the following documents, which are published on the school's official website in both Arabic and English, in accordance with the stipulations outlined in this Policy:

1. Digital strategy (see Section 2.1 Digital Strategy).
2. Responsible usage policies (see Section 4.1 Responsible Usage Policies).
3. Framework for the selection of external providers and products (see Section 5.4 External Providers and Products).
4. Data and Cybersecurity (see Section 6.1 Secure Digital IT Architecture).
5. Response plan in relation to cybersecurity incidents (see Section 6.6 Cybersecurity Incidents).
6. School data protection plan and policy (see Section 7. Data Protection).
7. Digital media policy and social media policy (see Section 8. Digital Communications).

2. Digital Strategy and Oversight

2.1 Digital Strategy: BRS has drafted and adopted a digital strategy that outlines and provides rationale for its digital goals over a 5-year time frame. The strategy includes:

1. Overall strategic direction on how technology shall be deployed to deliver better student achievement and outcomes (e.g., to enhance teaching and learning and to support the efficient and effective running of the school administration).
2. Assessment of how the school can use and provide assistive technology to enable inclusion.
3. Goals related to student digital skills and competencies that enable learning.
4. Development, procurement, and implementation plans for digital infrastructure, software, and hardware.

5. Mechanisms for ensuring the security of the school's digital systems.

6. Plan for future-proofing the school's digital infrastructure, where applicable.

7. Resources and investment required to deliver the digital strategy.

8. Staff training requirements.

9. Increase awareness related to emerging technologies (e.g., Artificial Intelligence).

2.2 Oversight: There is a Digital Wellbeing Committee which has the following responsibilities in relation to oversight of the school's digital strategy and associated policies:

1. Develop and implement the school's digital strategy.

2. Conduct an annual review of the digital strategy and its implementation:
   a. Monitor progress against student learning goals and school development and procurement plans.
   b. Evaluate technology, software, and online platforms to ensure that they meet the objectives of the strategy.
   c. Test and conduct risk assessments of the school's digital systems and infrastructure (e.g., backup recovery) to ensure that they are secure and fit for purpose.
   d. Review the effectiveness of the school's data and cybersecurity provisions.
   e. Re-evaluate the technological needs of the school based on feedback from staff, parents, and students, and plan procurement and digital development accordingly.
   f. Re-evaluate staff digital development needs and identify additional training required.

3. Develop and implement and review other school policies required to be created in line with this policy.

4. Engage with relevant stakeholders (e.g., the Digital Officer, Head of IT) to inform its decisions.

3. Digital Competencies

3.1 Student Outcomes: BRS ensures that the digital competencies and expected outcomes for students by grade are defined and these are integrated into the school's curriculum. Additionally, the school has the appropriate digital

infrastructure and resources in place to support students in achieving these outcomes, including students with additional learning needs, in line with the *BRS Inclusion Policy*.

3.2 Staff Training: BRS provides relevant training to staff in line with their designation to enable them to promote the objectives of this policy. The training covers topics such as the school's digital infrastructure and policies, student digital learning outcomes, data protection, cybersecurity, and the digital safety measures implemented by the school.

4. Responsible Usage and Digital Safeguarding

4.1 Responsible Usage Policies: BRS institutes and communicates responsible digital usage policies for students, parents, staff, and visitors. These policies set out what these groups are permitted/ prohibited to do on the school's premises, network, and systems, and include:

1. The definition of responsible usage of school software, network, services, and digital devices issued by the school, including shared devices.

2. Rules on the permitted and restricted use of personal devices on the school network and school premises, and during extracurricular activities that take place outside school (e.g., field trips).

    a. The school restricts the use of Virtual Private Networks (VPNs) by students on school premises or through school networks unless explicitly authorized for specific educational or administrative purposes.

3. Standards in relation to the use of personal social media accounts by staff (see Section 8.3. Personal Social Media Accounts for Staff).

4. The school's rules in relation to the setting and sharing of passwords for school accounts.

5. Standards in relation to the sharing of data related to the school or school community, and the channels via which such data can be shared when permitted. This includes standards related to the uploading of student data on external applications and learning tools, where applicable.

6. Standards in relation to academic honesty, plagiarism, and the responsible use of copyrighted material and digital tools (e.g., artificial intelligence), in line with the Federal Decree-Law No. (38) of 2021 on Copyrights and Neighboring Rights and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.

7. BRS communicates the relevant responsible usage policies to students, parents, staff, and visitors via appropriate channels.

    a. The school publishes responsible usage policies applicable to students and parents on the school website and in the Parent Handbook, as per the *BRS Parent Engagement Policy*.

    b. For all younger students up to Grade 6, the school provides age-appropriate versions of the policy to students, and a full version of the policy to parents.

42 Safeguarding Students: BRS puts in place education programs and effective systems to protect students from the online risks stated below.

1. Online risks posed to students are as follows:
    a. Exposure to content that is inappropriate, illegal, or may harm their wellbeing.
    b. Exposure to unsafe online interaction (e.g., interaction with users with fake profiles).
    c. Personal online behavior that can lead to harm for self or others (e.g., engaging in cyberbullying).
    d. Scams and finance-related risks such as gambling and phishing.

2. The school puts in place the following programs, systems, mechanisms, and procedures to safeguard students against online risks and promote their wellbeing:
    a. An age-appropriate awareness program for all students, covering the benefits of technology, awareness of online risks, self-assessment of online risks when using technology, online safety measures, and the impact of digital habits on wellbeing (e.g., the impact of duration of usage of digital devices).
    b. Appropriate filtering and monitoring systems to monitor student internet use on school devices and systems.
    c. Regular analysis of students' internet usage and web filter violations to identify potential adverse trends or problems.
    d. Procedures to identify and support students who appear to be developing risky, excessive, or illegal digital habits, such as digital addiction or gambling, in line with the *BRS Student Mental Health Policy* and the *BRS Student Behavior Policy*.
    e. Mechanisms to enable safeguarding during activities conducted virtually (e.g., disabling private chat for students).

3. BRS facilitates that there is a developmental purpose before allowing students to use the Internet during school hours.

4.3 Digital Incidents:

1. A digital incident occurs when a member of the school community engages in inappropriate use of digital technology. This includes a breach of reasonable usage policies, the accessing of inappropriate content, inappropriate behaviors or communications, cyberbullying, or any other breach of school regulations in an online setting.

2. Where a digital incident occurs during school hours or in settings covered in schools' digital policies, the school makes interventions and provide support to students and/ or staff in line with the relevant policy (e.g., *BRS Employment Policy*, *BRS Staff Wellbeing Policy*, *BRS Student Administrative Affairs Policy*, *BRS Parent Engagement Policy*, *BRS Student Behavior Policy*, and the *BRS Student Protection Policy*). Where required, the school will report digital incidents to ADEK and cooperate with the Abu Dhabi Police for investigations.

3. BRS safeguards that every digital incident is recorded, documented, and signed by the Principal and stored for auditing purposes, in line with the *BRS Records Policy*.

4.4 BRS urges its parents to monitor student s' usage of digital devices outside of school premises and school hours to ensure safe and appropriate digital behavior.

5. Digital Infrastructure

5.1 Digital Devices: BRS maintains that digital devices issued to members of the school community have appropriate security features and the school has defined and implemented digital safety precautions (e.g., minimum device specification, and antivirus requirements). The school allows its staff to access school-related data or systems on other devices and it has a Bring Your Own Device (BYOD) policy for staff or students.

5.2 Digital Systems for Staff: The schools ensures that relevant staff members have access to digital systems provided by ADEK, including the Learning Management System.

5.3 Distance Learning Readiness: BRS has adopted measures for distance learning for emergency situations such as temporary school closures or for individual students in exceptional circumstances (e.g., prolonged hospital stay, or emergency travel with parents for extensive periods).

5.4 Assistive Technology: BRS provides assistive technology to students with additional learning needs as indicated in their Documented Learning Plan, in line with the *BRS Inclusion Policy*.

5.5 External Providers and Products:

1. BRS has developed a third-party risk assessment framework for selecting external IT service providers and products related to the school network, system, and infrastructure, including learning application providers and open-source applications. This framework includes the following, at a minimum:

    a. Compatibility with existing school systems.
    b. Secure management of data.
    c. Compliance with cybersecurity standards and frameworks.
    d. Security against cyber threats.
    e. Service delivery and backup/ recovery provisions.
    f. Reputation and financial stability of the provider.
    g. Adherence of the vendor to the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and the ADEK terms and conditions,
    copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.
    h. Where relevant (e.g., learning application providers), educational quality, and age-appropriateness of content.

2. BRS communicates to external vendors that the vendor is subject to the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.

6. Data and Cybersecurity

6.1 Secure Digital IT Architecture: BRS has established a robust secure digital infrastructure and ensures the relevant cybersecurity controls are implemented as follows:

1. Access Control
    a. Implement multi-factor authentication mechanisms across critical services.
    b. Define and enforce role-based access control to ensure users have appropriate permissions.

2. Data Encryption
    a. Employ encryption for data in transit and at rest to safeguard sensitive

information.

3. Network Security
   a. Deploy next-generation firewalls and intrusion detection/ prevention systems to protect against unauthorized access.
   b. Ensure web filtering policies are enforced.
   c. Ensure the ability to block inappropriate content.
   d. Ability to detect infected machines across the school network.
   e. Ensure identity-based firewalls are implemented to provide granular visibility on user browsing activity.
   f. Established a unified security edge architecture for all internet browsing.
   g. Regularly monitor and audit network traffic for unusual patterns.

4. Endpoint Protection
   a. Install and update anti-virus/ anti-malware software on all school-managed devices.
   b. Implement hard disk device encryption and ensure regular security patching.

5. Data Backup and Recovery
   a. Establish automated regular backup procedures for critical data.
   b. Ensure backups are vaulted and stored offline.
   c. Develop a robust disaster recovery plan to minimize downtime in case of a security incident.

6. Data Security
   a. Establish data classification controls across school and student data.
   b. Implement Data Loss Prevention Tools to ensure data leaks or exfiltration is prevented.

7. Security Awareness Training
   a. Conduct regular training sessions for staff and students to raise awareness about cybersecurity threats and best practices.

8. Incident Response Plan
   a. Develop and regularly update an incident response plan to address security breaches promptly and effectively.
   b. Perform a tabletop cyber-attack simulation and exercise with school management involvement.

9. Physical Security
   a. Ensure secure access to physical servers, networking equipment, and other critical infrastructure.

10. Regulatory Compliance
    a. Ensure compliance with local and international data protection regulations and standards.

11. Monitoring and Logging
    a. Implement comprehensive monitoring systems to detect and respond to security incidents in real time.
    b. Maintain detailed logs for auditing and analysis purposes.

12. Secure Software Development
    a. Follow secure coding practices when developing or procuring educational software.
    b. Regularly update and patch software to address vulnerabilities.

13. Cloud Security
    a. If using cloud services, ensure the selected providers adhere to st ringent security standards.
    b. Implement proper configuration and access controls for cloud resources.
    c. Integrate Cloud Services – Software as a Service (SaaS) with school identity services where possible.
    d. Establish Cloud SaaS Security Posture Management capabilities.

14. Collaboration Security
    a. Secure communication and collaboration platforms to protect sensitive educational information shared among students and staff.

15. Third-Party Security
    a. Vet and monitor third-party vendors providing educational technology solutions to ensure they meet security standards.

6.2 System Maintenance: BRS maintains and regularly updates digital infrastructure, operating systems, security systems, and software, including antivirus protection software. The school regularly test its digital infrastructure and systems to ensure they are in good working condition.

6.3 Safe Use of External Learning Applications: BRS has have safeguarding mechanisms in place (e.g., single sign-on systems) to protect student and system security in the use of external learning applications.

6.4 Safe Virtual Interaction with Invited Visitors: BRS seeks parents' consent for any live virtual interactions with invited visitors, inside or outside of class. All such interactions are approved by ADEK, in line with the *BRS Extracurricular Activities and Events Policy* and the *BRS Student Protection Policy*.

6.5 Backup and Storage: Regarding the onsite data storage systems, BRS ensures that backups of important information, software, and configuration settings are performed at an appropriate frequency and retained for an appropriate period of time to allow for business continuity.

1. BRS ensures that such backups are stored securely and separately from the school network.

2. Regarding its external cloud systems for storage, BRS ensures that its data is synced to the cloud.

6.6 Cybersecurity Incidents: The school has developed response and business continuity plans to guide staff in the event of a cybersecurity incident, including the protocols for reporting the incident to the school leadership team and to ADEK, and the process for maintaining operational continuity.

1. The school does not communicate any cybersecurity incident to external parties except for the service provider involved and ADEK.

2. The school adheres to all applicable laws and policies set out by the Abu Dhabi Digital Authority and any other relevant authorities in the UAE, including the Federal Decree Law No. (34) of 2021 on Combatting Rumors and Cybercrimes.

7. Data Protection

7.1 Data Protection Policy: BRS has engineered a Data Protection Policy, setting out how the school ensures that personal information is dealt with correctly and securely, and in compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data, which includes, at a minimum:

1. The specification of the types of personal information that may be collected.

2. The requirement and procedures for individual consent in the collection, processing, and storage of personal information.
   a. Consent must be freely given, specific, informed, and unambiguous.
   b. Consent may be withdrawn by the individual at any time.

3. The conditions under which personal information may be shared by the school with other individuals or entities (e.g., with ADEK).
   a. BRS has a non-disclosure agreement built into any agreements with contractors in which personal data cannot be shared within or outside the country for any purposes, without the explicit consent of ADEK.

7.2 Sharing Data with ADEK: BRS is dutybound to provide accurate and up-to-date data

to authorized ADEK personnel on request, in line with the Federal Decree Law No. (18) of 2020 on Private Education and Law No. (9) of 2018 Concerning the Establishment of the Department of Education and Knowledge and in line with the ADEK terms and conditions, and data privacy policy with regard to the collection, use, and disclosure of information.

1. BRS will inform parents of their obligations to share data with ADEK accordingly.

7.3 Data Protection Plan: BRS has formulated and annually review a data protection plan, in compliance with Federal Decree Law No. (45) of 2021 on the Protection of Personal Data and the *BRS Records Policy*. The data protection plan sets out the steps taken by the school to safeguard its organizational data, including data classification methods, authorization levels, protections against cybersecurity and other threats, and procedures for restoring backed-up information in case of breaches.

8. Digital Communications

8.1 Digital Media Policy: BRS has implemented, and monitors a Digital Media Policy governing the creation and publication of digital media. The policy includes, at a minimum:

1. The requirement to obtain consent before recording and publishing digital media:
   a. The school only takes photographs and/ or video recordings of students after obtaining written consent from parents. In obtaining consent, the school informs parents about the purposes for which the photographs and/ or video recordings are being taken.

   b. The school also obtains written consent from parents before publishing digital content involving students. Additionally, the school clearly specify if the student will be identified by name in the publication when obtaining consent.

2. The procedures for the provision and withdrawal of consent.

3. Conditions related to the storage and security of digital media.

4. Conditions related to the use of personal devices and accounts for recording or publishing school content.

8.2 Social Media Policy: BRS has developed and implemented a Social Media Policy in relation to the use of social media by the school.

1. The policy includes, at a minimum:

a. Social media platforms and accounts to be used by the school.
b. Access, security, and password protection procedures for the school's social media accounts.
c. Conditions related to content, language use, and engagement with other accounts.
d. Conditions related to the use of names, photos, and videos of students, in accordance with Section 8.1. Digital Media Policy.
e. Guidelines for moderators (see Section 8.2.2. Moderators) in relation to content posted by third parties on the school's social media pages, including procedures to manage disrespectful content and trolling.
f. Procedures for addressing other adverse social media behaviors, such as impersonation of the school's accounts.

2. Monitoring School Communications: BRS regularly monitors all official and unofficial school-related communication channels (newsletters, social media, parent communication groups, etc.) to ensure its compliance with this policy.

3. Moderators: BRS has appointed moderator(s) to pre-approve or remove content posted by other users on the schools' social media pages, where possible, in line with the school's guidelines. Moderator(s) reject or remove, where possible, content that is inappropriate, not in line with the UAE cultural values, or amounts to bullying, harassment, discrimination, or intimidation, in line with the *BRS Values and Ethics Policy* and the *BRS Cultural Consideration Policy*.

83 Personal Social Media Accounts for Staff: The school has authorized members of staff to create and maintain existing personal social media accounts. In relation to these, staff members:

1. Do not use email addresses issued by the school to create such accounts.

2. Use the tightest possible privacy settings.

3. Do not identify themselves as being associated with the school, except on professional social media platforms (e.g., Linked In).

4. Do not accept invitations to friend, connect with, or follow from current students or former students under the age of 18, or send such requests to current students or former students under the age of 18.

5. Do not accept invitations from parents of current students to friend, connect

with, or follow them.

6. Do not use such accounts to communicate with current students, their parents, or former students under the age of 18. This applies to messaging applications (e.g., WhatsApp, Telegram, Signal).

7. Assume that content posted through such accounts (including online reviews and comments) is publicly visible and searchable, regardless of the privacy settings, and exercise appropriate discretion.

8. Ensure that content shared through such accounts is appropriate, in line with the *BRS Cultural Consideration Policy*, and does not amount to bullying, harassment, discrimination, or intimidation, in line with the *BRS Values and Ethics Policy*.

9. Ensure that content shared through such accounts does not give the impression of being endorsed by the school.

10. Ensure that they do not share any confidential information related to the school through such accounts.

84 Communications via Email: The school has informed staff members that they are not authorized to use personal email addresses to communicate with students or parents.

85 School Website: BRS has created a dedicated website and keeps it up to date to serve as a reference for members of the school community.

1. The school has published the following content on their website, at a minimum:
   a. Contact information.
   b. Services provided by the school.
   c. Fees, including transportation fees and fees for optional activities.
   d. Inspection reports.
   e. Aggregate student achievement data or individual achievements (e.g., awards), with consent.
   f. Public versions of the annual report, in line with the *BRS Reporting Policy*.
   g. School policies that are relevant to parents and/ or students.
   h. Any other required content, as defined by BRS policies.

2. The school ensures that the content published on its website is accurate and appropriate, in line with the *BRS Values and Ethics Policy*.

3. The school ensures that content published on its website is in line with the requirements for digital media (see Section 9.1. Digital Media Policy).

9. Compliance

9.1 This policy is effective as of the start of the Academic Year 2024/ 25 (Fall term). The school shall be fully compliant with this policy by the start of the Academic Year 2025/ 26 (Fall term).

Approved By:

Rachna Prakash
Principal
Bright Riders School-Abu Dhabi

Next Review: AY 2026-2027