FUTURE LEADERS
International Private School
Baniyas

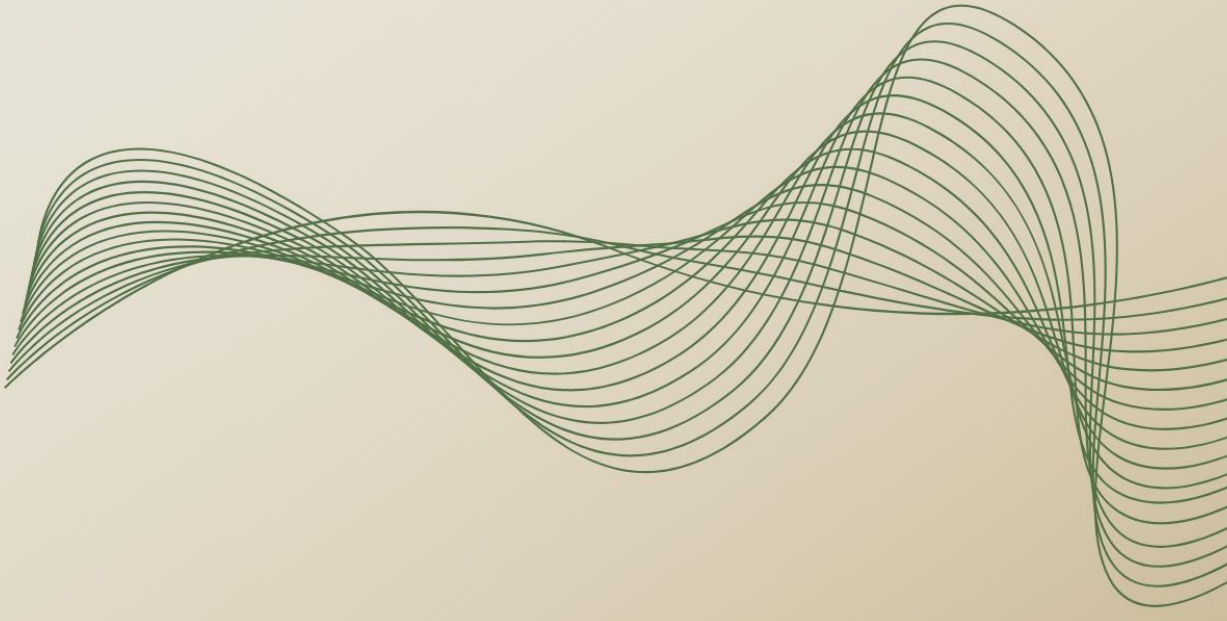
Digital Policy

Version 1
June 2024.

FUTURE LEADERS
International Private School

Baniyas

Approved by	Board of Trustees
Date of Review	June 2924
Next date of review	June 2025



1. Introduction:

In an era where technology pervades every aspect of education, Future Leaders International Private School is committed to ensuring the responsible and effective use of digital resources within our school community. Our Digital Policy encompasses a set of guidelines and protocols designed to enhance learning outcomes while prioritizing the safety and well-being of all stakeholders.

Our Digital Policy encompasses a set of guidelines and protocols designed to enhance learning outcomes while prioritizing the safety and well-being of all stakeholders. The digital policy integrates six key policies, each addressing specific aspects of digital usage and online conduct, thereby fostering a holistic approach to digital citizenship and responsible technology integration.

The policies included in our comprehensive Digital Policy are:

1. **Bring Your Own Device (BYOD) Policy and Acceptable Use Policy (AUP)**
2. **Data Protection and Privacy Policy**
3. **Online Safety Policy**
4. **Distance Learning Policy**
5. **Mobile Devices Usage Policy**
6. **Social Media Policy**

2. Purpose and Scope

Purpose:

To ensure the effective, responsible, and safe use of digital resources within the school community, enhancing learning while protecting all stakeholders.

Scope:

This policy applies to all students, staff, parents/guardians, and any individuals associated with Future Leaders International Private School who use the school's technology, data, network, and communication tools.

3.1. Bring Your Own Device (BYOD) Policy and Acceptable Use Policy (AUP)

Introduction:

In an era where technology pervades every aspect of education, Future Leaders International Private School is committed to ensuring the responsible and effective use of digital resources within our school community. Starting from the academic year 2024/2025, middle and high school students will be allowed to bring their own devices (BYOD) to school. This initiative aims to enhance the learning experience by providing students with greater familiarity with educational apps, easy access to learning resources, assignments, and study materials, and fostering digital literacy skills essential for their future academic and professional endeavors.

Purpose:

The Acceptable Use Policy (AUP) establishes clear guidelines for the appropriate use of technological devices and digital resources provided by Future Leaders International Private School or brought by the students (BYOD). The goal is to ensure these resources are used to enhance learning while maintaining a safe and respectful environment.

Scope:

This policy applies to all students, staff, and any other individuals using school-provided technological devices and digital resources, including but not limited to iPads, computers, and internet access. It also applies to personal devices brought by students for educational purposes.

BYOD Specific Guidelines:

Device Requirements:

Middle School: iPads

Device Options	iPad (8th generation) or later
Operating System	iPadOS 15 or higher
Storage Capacity	Minimum 64GB
Accessories	Protective case, keyboard case (optional), and Apple Pencil (optional)
Software	Necessary educational apps as specified by the school
Security	Up-to-date security settings and regular software updates
Network Compatibility	Ability to connect to the school's Wi-Fi network

High School: Laptops

Device Options	MacBook or Windows laptop
Operating System	MacBook: macOS 12 Monterey or higher Windows Laptop: Windows 10 or higher
Hardware Specifications	Processor: Intel Core i5 or higher RAM: Minimum 8GB Storage Capacity: Minimum 512 GB SSD Screen Size: Minimum 13 inches
Accessories	Protective case, external mouse (optional)
Software	Necessary educational apps as specified by the school
Security	Up-to-date security settings and regular software updates
Network Compatibility	Ability to connect to the school's Wi-Fi network

Educational Use Only:

Personal devices are to be used exclusively for educational purposes during school hours. Non-educational use, including gaming, social media, and streaming, is prohibited.

Classroom Use:

Devices may only be used in the classroom with the teacher's permission and must be relevant to the lesson or activity.

Security:

Students are responsible for the security of their personal devices. The school is not liable for lost, stolen, or damaged devices. It is recommended that devices be clearly labeled with the student's name.

Privacy and Respect:

Students must respect the privacy and rights of others. Taking photos or recording videos without permission is prohibited. All content accessed or shared on personal devices must adhere to school policies.

Network Access:

Students must use the school's Wi-Fi network for internet access during school hours. Using personal data plans to bypass school network restrictions is prohibited.

Technical Support:

The school's IT department will provide limited technical support for personal devices. Parents and students are responsible for maintaining their devices and ensuring they are in working order.

Compliance:

Students must comply with all other relevant school policies, including the Acceptable Use Policy (AUP), Online Safety Policy, Data Protection and Privacy Policy, and Distance Learning Policy.

Acceptable Technological Devices Usage:

Classroom Use: iPads and other devices provided by the school are for classroom use only, under teacher direction. Personal devices (BYOD) are to be used exclusively for educational purposes during school hours and only under teacher direction.

Camera and Microphone: Use of the camera and microphone is prohibited without teacher permission.

Recording and Posting: Students may not record, transmit, or post images or videos of others without their permission.

Content: Accessing, sending, or distributing offensive, threatening, or inappropriate materials is prohibited.

App Installation: Installing music or apps that violate copyright laws is not allowed on school-provided devices. On personal devices, only school-approved apps and software should be used during school hours.

Behavior: Cyberbullying, harassment, or disrespectful conduct is prohibited.

Language: Online language must be classroom-appropriate.

Curriculum Relevance: Access only files and sites relevant to the curriculum.

Security Issues: Report security or network issues immediately.

Personal Information: Do not reveal personal information online.

Jailbreaking: Jailbreaking (removing Apple-imposed limitations on the iPad) is prohibited**.**

Responsibilities:

Students:

- Use personal devices responsibly and in accordance with school policies.
- Report any misuse, technical issues, or security concerns to their teachers or the IT department.
- Ensure devices are charged and ready for use during school hours.

Parents:

- Ensure devices meet school requirements and are properly maintained.
- Monitor their children's device usage at home and support the school's BYOD policy.
- Assist with installing required software and security updates.

Teachers:

- Integrate personal devices into the curriculum where appropriate and supervise their use.
- Report any misuse or technical issues to the IT department.
- Promote responsible and ethical use of technology in the classroom.

IT Department:

- Provide guidance on device requirements and limited technical support.
- Ensure the security of the school's network infrastructure.
- Offer training sessions for students, parents, and staff on proper device usage and cybersecurity.

Consequences of Violations:

Violations of the AUP and BYOD policy may result in disciplinary actions, including:

- Verbal or written warnings
- Temporary suspension of BYOD privileges
- Confiscation of the device for the school day
- Parental meetings
- Other measures deemed appropriate by school administration

Communication and Updates:

The school will regularly communicate any updates or changes to the AUP and BYOD policy to parents and students. Feedback will be solicited to ensure the policy remains effective and relevant. Additionally, annual reviews will be conducted to align the policy with technological advancements and emerging issues.

3.2. Data Protection and Privacy Policy

Purpose:

The purpose of the Data Protection and Privacy Policy is to safeguard the personal data of students, staff, and other stakeholders associated with the school and to ensure compliance with relevant data protection laws and regulations. By establishing clear guidelines and procedures, this policy aims to protect individuals' privacy rights and promote trust in the school's handling of personal data.

Scope:

This policy applies to all personal data processed by the school, encompassing data collection, storage, and sharing activities. It applies to all individuals, including students, staff, parents, and any other parties whose personal data is processed by the school.

Responsibilities:

It is the responsibility of all school staff members to handle personal data in accordance with this policy and relevant data protection laws. Staff members must ensure that personal data is processed lawfully, fairly, and transparently, and that appropriate measures are taken to protect it from unauthorized access or disclosure.

Data Collection and Use:

Consent: The school shall obtain explicit consent from individuals before collecting their personal data, except where otherwise permitted by law.

Purpose Limitation: Personal data shall be collected only for specific, legitimate purposes and shall not be further processed in a manner incompatible with those purposes.

Data Minimization: The school shall collect and process only the personal data that is necessary for the intended purpose, and shall ensure that it is accurate and up to date

Data Security:

Storage: Personal data shall be stored using secure storage solutions to prevent unauthorized access, loss, or damage.

Access Control: Access to personal data shall be restricted to authorized personnel only, and appropriate access controls shall be implemented to prevent unauthorized access.

Rights of Individuals:

Access: Individuals have the right to access their personal data held by the school and to request information about how it is being processed.

Correction: Individuals have the right to request the correction of inaccurate or incomplete personal data.

Deletion: Individuals have the right to request the deletion of their personal data under certain circumstances, such as when it is no longer necessary for the purposes for which it was collected.

Compliance:

The school shall regularly review and update its data protection practices to ensure compliance with this policy and relevant data protection laws.

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or enrollment, as appropriate.

This policy shall be communicated to all relevant stakeholders and made readily accessible to individuals whose personal data is processed by the school.

3.3. Online Safety Policy

Purpose:

The purpose of this Online Safety Policy is to ensure that all members of the school community at Future Leaders International Private School are provided with a safe and secure online learning environment. This policy aligns with the Students Well-Being Policy, Child Protection Policy, Anti-Bullying Policy, Acceptable ICT Use Policy, and Health and Safety Policy to create a comprehensive approach to online safety and aims to protect students, staff, and other stakeholders from online threats, cyberbullying, and misuse of digital resources while promoting responsible and ethical use of technology.

Scope:

This policy applies to all students, staff, parents/guardians, and any other individuals or organizations associated with Future Leaders International Private School who use the school's online resources, networks, and communication tools. It covers the use of school-provided devices, personal devices on school property, and all online interactions that involve members of the school community.

Responsibilities:

School Principal: Policy development, implementation, compliance, support, and monitoring.

Online Safety Coordinator: Policy creation, implementation, daily issue management, training, and awareness.

IT Department: Secure infrastructure, up-to-date software, confidentiality, and monitoring.

Students: Adhere to the policy, report concerns, and use devices responsibly.

Parents: Support the policy, ensure safe device use at home, attend training, and encourage responsible behavior.

Teachers: Integrate online safety education, supervise online activities, and report concerns.

Online Safety Measures:

Filtering and Monitoring: Employ filters to restrict access to inappropriate content and monitor online activities.

Cyberbullying Prevention: Enforce a zero-tolerance policy with swift investigation and appropriate action.

Data Privacy: Safeguard privacy in compliance with relevant laws and regulations.

Incident Reporting: Encourage timely reporting of incidents, including anonymous reporting options.

Education and Awareness: Provide ongoing education to cultivate responsible online behavior among all stakeholders.

Consequences of Violations: Violations may result in disciplinary actions, including loss of access to online resources, devices, and networks.

Promotion of Digital Citizenship:

The school will actively promote digital citizenship by providing helpful tips, videos, and resources to parents to support their understanding of digital literacy and responsible online behavior. Additionally, the school will organize workshops and training sessions for teachers and students to enhance their knowledge and skills in digital citizenship. These workshops may cover topics such as online safety, privacy protection, cyberbullying prevention, and critical thinking in the digital age.

3.4 Distance Learning Policy

Purpose:

The purpose of the Distance Learning Policy for Adverse Conditions and Pandemics is to ensure continuity of education during circumstances such as inclement weather, heavy rain, or pandemics when traditional in-person schooling may be disrupted.

This policy aims to provide guidelines for the seamless transition to remote learning, utilizing digital platforms such as Zoom and Microsoft Teams, to facilitate uninterrupted educational experiences for students, supported by prepared teachers, encouraged by parents, and supervised by school staff.

Activation of Distance Learning:

- During pandemics or health crises, or in the event of adverse weather conditions, heavy rain, or other circumstances preventing physical attendance at school where in-person schooling is not feasible or safe, the distance learning protocol will be implemented as per the recommendations of relevant health authorities.

- The school administration will share information with parents regarding specific days when learning will be conducted online, following directives from the Abu Dhabi Department of Education and Knowledge (ADEK) circulars or guidelines.

Digital Platforms:

- The school will utilize digital platforms such as Zoom and Microsoft Teams for conducting remote classes and maintaining academic continuity.

- Teachers will be provided with necessary training and resources to effectively use these platforms for remote teaching.

Attendance and Participation:

- Students are expected to join remote classes at the scheduled times, following their regular school timetable.

- Parents are encouraged to support and encourage their children to actively participate in remote learning activities and ensure a conducive learning environment at home.

- School supervisors will monitor class attendance and student participation during remote sessions.

Preparedness of Teachers:

- Teachers are responsible for preparing and delivering engaging and interactive remote lessons, utilizing appropriate digital resources and teaching methods.

- Teachers should ensure that learning materials are accessible to students through digital platforms and provide necessary support and guidance as required.

Communication and Support:

- The school will maintain open channels of communication with parents, providing regular updates and guidance regarding remote learning activities and expectations.

- Parents can reach out to teachers or school administrators for assistance or clarification regarding remote learning arrangements.

Review and Improvement:

- The school administration will regularly review and evaluate the effectiveness of the distance learning policy and make necessary adjustments based on feedback and lessons learned from implementation.

- Feedback from students, parents, teachers, and staff will be solicited to identify areas for improvement and ensure continuous enhancement of the distance learning experience.

3.5. Mobile Devices Usage Policy

Purpose:

The purpose of the Mobile Devices Usage is to establish clear expectations for the appropriate use of mobile devices during school-sponsored events and trips. By providing guidelines focused on responsible digital behavior, the aim is to ensure that mobile devices are utilized purposefully to enhance the educational experience, promote safety, and respect the privacy and rights of all individuals involved.

Scope:

These guidelines apply to all students participating in school events and trips where the use of mobile devices is permitted. They outline specific expectations regarding the use of mobile devices for capturing event-related memories, respecting privacy, engaging in school-related activities, avoiding inappropriate content, adhering to designated usage hours, ensuring device security, and compliance with all school policies.

Guidelines:

Purposeful Photos: Capture event-related memories only.

Respect Privacy: Obtain permission before taking photos of others.

Responsibility: Use devices for school-related activities only.

Inappropriate Content: Do not engage in taking or sharing inappropriate content.

Time and Place: Use devices only during designated hours.

Security: Secure devices against loss or theft; the school is not responsible for damages.

Follow Policies: Adhere to all school policies.

Student Acknowledgment: Students must read, understand, and agree to these guidelines, with consequences for non-compliance.

3.6. Social Media Policy

Purpose:

The purpose of the Social Media Policy is to provide guidance on the responsible and appropriate use of social media by students, staff, and the school community. This policy aims to uphold professional standards, protect privacy and confidentiality, and maintain a positive online presence that reflects the values of the school.

Scope:

This policy applies to all social media use related to the school, including posts on official school accounts and mentions of the school on personal accounts. It encompasses interactions on various social media platforms, including but not limited to Facebook, Twitter, Instagram, and LinkedIn.

Guidelines:

Professionalism: All social media interactions related to the school should maintain a professional tone and adhere to the highest ethical standards. Respect for privacy and confidentiality must be maintained at all times.

Representation: Only authorized personnel designated by the school administration may post on behalf of the school. These individuals are responsible for ensuring that all content shared accurately represents the school's values and objectives.

Content: Users are prohibited from posting any content that is inappropriate, offensive, or confidential. This includes but is not limited to defamatory statements, discriminatory remarks, or any content that violates the rights of others.

Engagement: Users are encouraged to engage in positive interactions and promote constructive dialogue. Any negative comments or issues should be addressed promptly and professionally, either publicly or through direct messaging where appropriate.

Parental Consent for Student Photos:

At the beginning of each academic year, the school will seek permission from parents or legal guardians before sharing any photos of students on social media platforms for school activities and educational purposes. This consent will outline the specific purposes for which the photos may be used and provide parents with the option to opt-out if they do not wish for their child's photo to be shared.

Consequences of Violations:

Violations of this policy may result in disciplinary actions, which could include the suspension of social media privileges, formal reprimands, or other measures deemed appropriate by school administration. Repeat offenses may result in more severe consequences, up to and including termination of employment or enrollment.

Compliance:

All members of the school community are expected to familiarize themselves with this policy and adhere to its guidelines. The school administration will periodically review and update this policy to ensure its effectiveness and relevance in an evolving social media landscape.

4. Staff Professional Development

Purpose:

The purpose of Staff Professional Development is to empower staff members with the necessary knowledge and skills to effectively utilize and manage digital resources, while also promoting online safety within the school community. By providing comprehensive training and support, this initiative aims to enhance staff confidence in leveraging technology for educational purposes and ensure a safe and secure online environment for all stakeholders.

Components:

Training Programs: The school will conduct regular workshops and training sessions focused on various aspects of digital literacy, including but not limited to new technologies, online safety, cybersecurity, and responsible digital citizenship. These sessions will be tailored to meet the specific needs and interests of staff members, ensuring that they are equipped with the latest tools and strategies to enhance their professional practice.

Support: In addition to formal training programs, staff members will have access to ongoing support and resources to stay updated on digital trends and best practices. This support may include online tutorials, informational materials, peer mentoring, and consultation services from technology experts. The school will also encourage collaboration and knowledge sharing among staff members to foster a culture of continuous learning and innovation.

Evaluation: The school will implement regular assessments to evaluate staff proficiency and identify areas for further development in digital literacy. These assessments may take the form of surveys, self-assessments, performance reviews, or practical demonstrations of skills. Based on the results of these evaluations, the school will tailor future training programs and support initiatives to address specific needs and challenges identified by staff members.

By investing in staff professional development in digital literacy, the school aims to cultivate a dynamic learning environment where staff members are empowered to harness the full potential of technology for educational excellence while prioritizing the safety and well-being of all individuals in the school community.

5. Reporting and Responding to Technology Misuse and Inappropriate Behavior

Reporting Incidents:

Students: It is imperative for students to promptly report any instances of technology misuse or inappropriate behavior to their teachers, supervisors, or the designated online safety coordinator. This can be done through designated reporting channels established within the school's communication systems.

Teachers: Teachers are responsible for documenting and reporting incidents of technology misuse or inappropriate behavior to the online safety coordinator. They should maintain detailed records of the incident, including relevant evidence such as screenshots or written accounts.

Administrators: Upon receiving reports of incidents, administrators are tasked with conducting thorough and confidential investigations. This involves gathering evidence, interviewing relevant parties, and assessing the severity and impact of the incident.

Responding to Incidents:

Initial Assessment: An initial assessment is conducted to determine the severity and impact of the incident. This helps in formulating an appropriate response and implementing necessary interventions.

Notification: Parents or guardians of the students involved in the incident are promptly informed. Transparent communication is maintained throughout the process to keep them informed of the situation and any actions being taken.

Disciplinary Action: Depending on the nature and severity of the incident, disciplinary actions may vary. Consequences for technology misuse or inappropriate behavior may include verbal warnings, written warnings, parental meetings, temporary suspension of iPad privileges, or other corrective measures. Repeat offenses may lead to more severe disciplinary actions in accordance with the school's disciplinary policy

Legal Compliance: In cases where the incident involves illegal activities or serious breaches of conduct, the school will cooperate fully with legal authorities as necessary. This includes providing necessary information and assistance to law enforcement agencies or relevant authorities.

Education and Awareness:

Programs: The school actively implements programs aimed at promoting responsible technology use and preventing cyberbullying. These programs may include workshops, seminars, guest speakers, and educational materials designed to educate students, parents, and staff on safe and ethical online behavior.

Professional Development: Ongoing professional development opportunities are provided to teachers to enhance their skills in monitoring and guiding students' technology use. This includes training sessions focused on identifying signs of misuse, responding effectively to incidents, and integrating digital citizenship principles into the curriculum.

6. Annual Review and Policy Updates

Purpose:

The purpose of the Annual Review and Policy updates is to maintain the relevance and effectiveness of all digital policies in addressing emerging issues and technological advancements.

Process:

Review: Conduct annual reviews of all digital policies to assess their efficacy and relevance.

Feedback: Gather feedback from students, staff, and parents to identify areas for improvement and address emerging concerns.

Revision: Update policies based on feedback, changes in technology, and emerging threats.

Approval: Policy updates to be reviewed and approved by the school principal and governing board to ensure alignment with the school's mission and values.

By adhering to this robust process of review and policy updates, Future Leaders International Private School aims to cultivate a secure, productive, and responsible digital environment for all members of the school community.