Digital Policy

Approved by:

Aysha Juma Al Khateri
Chairwoman

Date:

12/11/2025

Effective Date:
17/11/2025

Revision History

Revision Date	Version Number	Revised By	Signature
30/05/2025	02	Eva Sanchez Castillo Principal	

Data and Cybersecurity Infrastructure

School landline : 02 31 01 888 School P.O Box: 63797
www.spanishschool.ae info@spanishschool.ae

1. Introduction

The Spanish School of Abu Dhabi has the responsibility to ensure that every student in its care is safe whether in the digital world or the real world. The school is aware that IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods. New technologies are continually enhancing communication, the sharing of information and learning, social interaction and leisure activities.

However, we are also alert to the fact that they also pose great and more subtle risks to young people. Our students are, therefore, taught how to stay safe in the online environment and how to avoid risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalization.

This Data and Cybersecurity Infrastructure Policy establishes the controls required by the Abu Dhabi Department of Education and Knowledge (ADEK Digital Policy), the UAE Personal Data Protection Law (Decree-Law No. 45 of 2021), and other applicable standards. It provides a structured framework to secure our digital environment, preserve the confidentiality, integrity, and availability of information assets, and maintain the trust of students, parents, staff, and regulators.

2. Objective

This policy—reinforced by the Responsible Usage Policy for staff, students, parents, and visitors—exists to safeguard the entire school community by outlining practical measures to minimise online risks, address any infringements, and cultivate informed, responsible use of internet technologies. It ensures that every user understands the spectrum of digital threats, while actively educating students on e-safety so they remain secure and compliant with the law both inside and outside the classroom; it further promotes open dialogue in which students can voice their concerns and anxieties about online safety.

3. Scope

This policy sets This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems:

- **Staff** includes teaching and non-teaching staff and regular volunteers.
- **Parents** includes students' caregivers and guardians.
- **Visitors** includes anyone who is visiting the school, including occasional volunteers.

The Infrastructure policy along with Responsible Usage Policy for all staff and students, cover both fixed and mobile internet devices provided by the school such as PCs, laptops, webcams, tablets, smartboards, digital video equipment, etc. as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

4. Roles and Responsibilities

Principal

- Approves this policy and reviews its effectiveness at least once a year, or sooner if technology or regulatory requirements change.
- Ensures all staff are aware of, and adhere to, the school's E-Safety and Cybersecurity policies and procedures.

IT Department

- Translates this policy into day-to-day technical controls (e.g., access management, network protection, backups, monitoring, incident response).
- Maintains and regularly updates all digital infrastructure—including firewalls, endpoint protection, patch management, and secure configurations—to align with ADEK and UAE data-protection standards.
- Monitors system logs and security alerts, investigates potential incidents, and reports breaches to the Principal and relevant authorities in accordance with the Incident Response Plan.
- Conducts annual policy and infrastructure reviews, recommending improvements to the Principal to keep pace with evolving threats and technologies.

Students

- Use the school's IT systems responsibly and in full accordance with the E-Safety policy.
- Demonstrate understanding of the school's E-Safety protocols and immediately report any security concerns or inappropriate content to a teacher or the IT Department.

Parents / Guardians

- Actively promote safe and responsible technology use at home, reinforcing the school's guidelines.
- Support the school by endorsing the E-Safety and safeguarding policies, and by cooperating with any related initiatives or investigations.

5. Education and Training

Staff – awareness and training

- New staff receives information on the school's policies as part of their induction.
- All staff receive regular information and training on E-Safety issues through internal training and meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety.
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviors in their classrooms and following school procedures.

- Teaching staff are encouraged to incorporate E-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.
- When children are using school computers, staff make sure children are fully aware and are following the school's IT guidelines.
- Staff understands what to do in the event of misuse of technology by any member of the school community.
- The school staff understands their responsibilities to report online-cybersecurity incidents.
- The school encourages all users to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; Incident report flow chart is in place and understood so that processes are followed promptly.
- The school has the provision to seek support from other outside agencies in dealing with online-Safety issues in case there is a need.
- The school conduct regular training sessions for staff and students to raise awareness about cybersecurity threats and best practices.

Students

- IT and online resources are used increasingly across the curriculum. The school provides guidance to students about E-Safety within a range of curriculum areas and IT lessons and through presentations, workshops, assemblies on a regular and meaningful basis. The school continuously monitors and assesses students' understanding of it.
- At age-appropriate levels, students are taught about their E-Safety responsibilities and to look after their own online E-Safety risks (including recognizing online exploitation, stalking and grooming), and of their responsibility to report any such instances they or their peers come across.
- The school encourages all users to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes. Incident report flow chart is in place and understood so that processes are followed promptly.
- Students are taught about respecting other people's information and images.
- Students are aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy).

Parents

- The school seeks to work closely with parents in promoting a culture of E-Safety.
- The school contacts parents if it has any safety concerns about students' behavior while using technology online. Parents are guided and informed likewise to share any concerns, which they identify with the school.
- The school arranges training sessions/workshops for parents advising them about E-Safety and the practical steps that they can take to minimize the potential dangers to their ward, without curbing their natural enthusiasm and curiosity. These are done by both in-house trainers and specialist from outside.

6. *Password Security*

All users are responsible for maintaining the security of their login credentials and passwords. Passwords must adhere to the school's complexity requirements. Passwords must not be shared with anyone. User logins and passwords serve as a primary security measure to restrict access to the school network and online platforms, including Microsoft Office applications, Google Applications, Apple and Additio. If a password is compromised, it could allow unauthorized individuals to gain access to sensitive systems and data.

Users with logins are responsible for safeguarding against unauthorised access to their account, and as such, must ensure passwords are kept confidential. All passwords should be designed to be complex and difficult to breach.

Below are the systems or portals that can be logged in:

- School computers – for both staff and students.
- SSAD-EMPLOYEE WIFI network – for staff only.
- SSAD-STUDENTS WIFI Network – For school owned students devices (school iPads and iMacs),
- SSAD-GUEST WIFI Network -Guest users visiting school,
- Cambridge – staff and students,
- ABT – staff and students,
- NWEA MAP – staff and students,
- Slack – staff,
- Canva – staff and students,
- Kid A-Z – staff and students,
- Anaya – staff and students,
- Tekman – staff and students,
- STEAM – staff and students,
- Edpuzzle – staff and students,
- Kutubee – staff and students,
- Alef – staff and students,
- Abjadyat – staff and students,
- Office 365 – staff and students,
- Google Workspace– staff and students,
- Apple ID– staff and students,
- Additio – for both staff, students, and parents,

Users can change their password directly from a school owned computer if they know their current password.
In iMac & Macbook: From System preference > users and groups > change password.

In Windows: Press ctrl + Alt + Delete > select change password.
In Ipad: from Settings > Touch ID & Passcode > Change Passcode.

All users and system passwords should meet the following characteristics:

- Be at least 8 characters in length,
- Consist of a mix of alpha, and at least one numeric, and special symbols,
- Not be portions of associated account names (e.g., user ID, log-in name),
- Not be character strings (e.g., ABC or 123),
- Not be simple keyboard patterns.
- Passwords must be changed at least every 90 days. Previously used passwords cannot be re-used.

It is the responsibility of the end user to ensure enforcement with the policies above. If you believe your password has been compromised or if you have been asked to provide your password to another individual, immediately change your password and promptly notify IT Department
it@spanishschool.ae – 023101889

7. Authentication

if a student forgets a password, he\ she should inform their classroom teacher, who will submit the request to the IT Department on their behalf. Password reset email requests from students will be ignored and replied with the message 'forward through homeroom teacher'.

Staff can submit a request IT support for a password reset from their personal emails. However, the new IT provided password should change after signing in.

Staff logins are secured with multi-factor authentication from (MFA) Microsoft, Google and Apple. All the staffs' personal devices are registered in Microsoft, Google and Apple cloud. The user needs to authenticate their device for a successful login to email and online portals. System fails to sign in will occur in the absence of successful authentication.

8. Filtering

is important to note, that any filtering service, no matter how thorough, can never be comprehensive. Therefore, the school has a clearly understood policy on acceptable use for all users and adequate supervision is maintained.

The schools Wi-Fi and infrastructure has been installed and is maintained with an active, monitored filter system to satisfy both the needs of child protection/inappropriate content whilst ensuring that it serves to support teaching and learning. If at any time school staff or students find themselves able to access

internet sites from within school which they think should be blocked, they are advised to report the matter to the IT Department to handle such issues.

System

The Spanish School safeguards its network with a dual-layer solution: an on-premises Fortinet FortiGate next-generation firewall protects all internal traffic, while Securly's cloud-based filtering gateway secures school-issued devices when they are used off-site. Both platforms are configured with stringent security and content-filtering policies, collectively shielding our IT usage and infrastructure from unauthorised access, malware, and inappropriate online content.

Fortinet FortiGate firewall

The Spanish School's Fortinet FortiGate firewall blocks the website categories below for every user on the campus network. The rule-set is powered by live FortiGuard threat-intelligence feeds and is reviewed each term to ensure continued relevance to safeguarding requirements and ADEK guidance.

Category	**Content Blocked**
Adult & Explicit	Pornography, nudity and risqué material, lingerie/swimsuit sites, other adult materials, dating sites.
Violence & Weapons	Explicit or graphic violence, sports-hunting and war-game content, weapons sales or instructions.
Hate, Extremism & Terrorism	Extremist groups, hate or discrimination sites, terrorist content, advocacy organisations that promote illegal activity.
Child Protection	Child sexual-abuse imagery or forums.
Drugs, Alcohol & Tobacco	Illegal drug abuse, marijuana promotion, misuse of prescription drugs, alcohol and tobacco sales or advocacy.
Illegal or Unethical Activity	Hacking tutorials or tools, plagiarism resources, criminal-skill sites, illegal download portals.
Proxy & Evasion	Proxy-avoidance services, anonymisers, Dynamic DNS domains used to bypass filtering, crypto-mining sites.
Gambling	Online casinos, sports betting, lottery sites, gambling advice.
Malicious & Spam	Phishing pages, malicious websites, spam URLs, command-and-control domains.
Sensitive Social Issues	Abortion or alternative-belief sites deemed age-inappropriate for the student body.
Games (non-educational)	Online gaming portals that are not part of the curriculum.

Override & Escalation Procedure

- Staff request for access: A teacher needing a blocked resource for legitimate educational purposes submits a ticket to the IT Department with a brief rationale.
- Safeguarding review: The IT Department and Coordination team review the request, consult curriculum leads if necessary, and either approve a temporary whitelist or suggest alternative material.
- Unexpected access: If any user discovers inappropriate or malicious content that has slipped through the filter, they must immediately report it to a member of staff, who will escalate to the IT Department for prompt investigation and rule adjustment.

Access to Network

Access to the network is provided through Firewall Radius Authentication. Access is therefore governed by device registration and approval by authorized staff only. No devices can join the network without this approval and authentication.

Hardware and General Service Provision

The following has been installed and configured in school to ensure only appropriate content is available to all users:

- School licenses are purchased on a fixed one-year term to ensure continuity of service, and the individual firewall is monitored 24/7 with instant notification of any concerns.
- A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented.
- The firewall appliance is configured for the Global view Internet filtering service, powered by Fortinet. The service is a professional, commercial category-based web-filtering solution and is used in many organizations worldwide.
- It uses a category-based system to group web sites in addition to keyword, IP and specific white and blacklist control.
- In addition, IP and URL black- and whitelisting is supported locally which ensures any content that is flagged as non-desirable on the network, can be disabled immediately.
- Access logs are maintained for all traffic and all attempts at access of inappropriate content.

Specifics of Filtering Service

- Fortinet independently searches the Internet using their tools to select what category is assigned to any available website. This is matched to the live filtering within the school
- If a website falls into a category that is not deemed acceptable for use in the classroom, the user gets an “blocked” notification on the web browser and this activity is logged to user and device level.
- Filtration service uses a category-based system to decide if a website is viewable from all Internet connected devices. The primary Categories include:

- Computer & Internet Services (spam sites)
- Child Protection (including child sexual abuse; extreme pornography or criminally racist or terrorist content)
- Other (dating and person)

Securly Cloud-Based Filtering

To protect and monitor school-issued laptops, and Lab iMacs when they leave campus, The Spanish School deploys Securly's cloud DNS/proxy filter and device agent. The service applies the same safeguarding standards enforced on-site by Fortinet, while adding AI-driven monitoring for student safety keywords (self-harm, bullying, violence). Policies are synchronised from a central console and updated every few minutes from Securly's threat-intelligence network.

Category	**What Is Blocked**
Pornography	Sexually explicit images, videos, or text; full nudity.
Drugs	Information or promotion of prescription or recreational drug use.
Gambling	Online casinos, betting, lotteries, gambling advice.
Other Adult Content	Mature themes such as violence, alcohol, graphic imagery, lingerie.
Social Media	Media-sharing communities with user-generated content.
Social Networking	Sites for building personal/professional relationships.
Network Misuse	Anonymisers, piracy streams, hacking or translation loopholes.
Chat / Messaging	Web-based instant-messaging platforms.
Intolerance	Hate or discriminatory content targeting protected groups.
Other Search Engines (No Safe Search)	Search engines lacking enforceable Safe Search.
Streaming Media	Audio/video services that can distract from learning.
Games	Online single- or multiplayer gaming sites.
Health	Medical advice or detailed human-anatomy content.
Uncategorized (Browser Extension)	Sites not yet classified—blocked only by the browser plugin.
Uncategorized (SmartPAC)	Unscanned sites—blocked if SmartPAC is in use.

Malware	Domains known to host malicious software.
E-commerce / Shopping	Online stores that may expose students to adult items.
Sexual Content (Non-Porn)	Sexual-health or advice sites without explicit imagery.
Plagiarism	Tools or repositories that facilitate academic dishonesty.
Web Ads	Ad networks known for inappropriate imagery or scams.

Additional Student-Safety Features

- AI Keyword Alerts: Securly scans searches, social posts, and emails for self-harm, bullying, or violence; high-risk alerts are sent instantly to designated safeguarding staff.
- Reports: weekly summaries of their child's off-site browsing, encouraging a shared approach to digital safety.
- Tamper Protection: Device agents prevent students from uninstalling the filter or using rogue VPN extensions.

9. Technical Security

Objectives

- Detect, prevent, and minimise the impact of virus or malware outbreaks on servers, desktops, and laptops.
- Contain or eradicate malicious code before it can spread throughout the network.
- Establish clear control measures and user responsibilities to maintain a secure operating environment.
- Ensure protection mechanisms run with minimal performance impact so users work effectively without undue delay.

Updates

periodic updates will be installed centrally over our servers/networking devices or physically by the IT staff in school owned computers and laptops

McAfee Software

The Spanish School secures every Windows and macOS endpoint with McAfee Endpoint Security (ENS), centrally administered through McAfee ePolicy Orchestrator (ePO). All configuration, signature distribution, and alerting are handled from the ePO console, allowing the IT Department to enforce consistent policies, push rapid updates, and maintain a real-time view of the school's malware posture.

ENS provides always-on, on-access scanning for files, network shares, email attachments, and removable media. To ensure the most current protection, virus definition (DAT) and engine updates are downloaded from McAfee Global Threat Intelligence every four hours and automatically propagated to all devices; any computer that misses two consecutive update cycles generates an alert for immediate remediation. In addition to traditional signature defence, the Adaptive Threat Protection module uses machine-learning and behavioural analytics to block ransomware, file-less attacks, and malicious PowerShell or macro activity before it can execute.

Full-disk scans run each Friday evening after school hours, while quick scans execute daily at midday to catch emerging threats without disrupting lessons. Where curriculum-critical software could be affected, the IT Department applies carefully scoped scan exclusions to maintain classroom performance without sacrificing security.

All USB storage devices and other removable media are automatically scanned on insertion; unapproved or encrypted media is blocked unless explicitly whitelisted. Users are prohibited from disabling McAfee services or ignoring warning pop-ups, and must report any suspicious activity to the IT HelpDesk immediately.

High-severity detections generate instant ePO alerts and email notifications to the IT Department. Multiple correlated infections trigger the school's Incident Response Plan, ensuring swift containment, investigation, and reporting in line with ADEK requirements.

McAfee policies are assessed each term to refine exclusions, scan schedules, and heuristics in response to evolving threat trends and user-experience feedback, ensuring that robust protection is delivered with minimal impact on teaching and learning.

Anti-Virus Policy

The school follows the below preventive and detective control measures to protect against malicious software and virus attacks;

- Scanning for Viruses.
- Users are allowed to use only authorized/licensed software in the school or while using the school intranet. Use of any other software without the permission the IT department is prohibited.
- All files and software downloaded/received either from or via external networks, e-mail, or on any other medium such as data storage media should be first scanned for viruses/ malicious code prior to its use.
- Database/file servers where critical data is stored is scanned for viruses on a regular basis.
- Any data storage media brought into the organization must be scanned for virus before being used by the user or to be given to the Information Security Team for scanning.
- School Laptops for users are first updated with the Anti-virus software and scanned for viruses by the information security team and approved, before connecting to the school network.

Desktop and Lapotop Usage

The school's desktop and laptop programme is designed to promote the responsible and secure use of all information-system assets. Every employee who is issued a device is expected to exercise a high level of care to safeguard both the hardware and the data stored on it. To that end, devices are allocated only after formal authorisation by the relevant department manager, and they are reclaimed when the employee departs the school, when a contract ends, or at the manager's written request. Robust security controls—such as full-disk encryption and remote-wipe capability—ensure that, in the event a laptop is lost or stolen, the only loss to the organisation is the physical hardware itself, not the sensitive information it once contained.

Statements

- Users must safeguard their Desktop/Laptop against loss, theft or damage.
- Users must lock their account when leaving the Desktop and/or Laptop unattended.
- Users must take care to safeguard Information Assets when accessing the IT Infrastructure from a public place.
- Users must backup their business-related files that they store on their Desktop and/or laptop on a regular basis on their Cloud backup folder.
- Users must not tamper with the administrative functions of the Desktop and/or Laptop such as its Operating System or Administrator identification and password.
- Users must use the school request and approval procedures for requesting the installation of external devices such as printers, storage devices, and third-party software to their Desktop and/or Laptop.

Terms and Compliance

- All users are responsible to safeguard the Desktop/Laptop issued to them and any stored Information Assets on it.
- In the event of loss of a laptop, users must report the loss to IT Department at school immediately, in order to limit the access to school systems.
- The IT team must investigate the circumstances of the loss of a laptop before a replacement is issued to the user.
- In case of non-compliance to this policy, disciplinary actions will be issued by the Information Technology division and reported to the Manager of the concerned department.

10. Use of Internet and Email

Staff

- Staff must not access any website or personal email, which is not connected with schoolwork or business whilst teaching / in front of students. Such access may only be made during non-contact time with the students.
- Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.
- The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.
- Staff must immediately report to IT and HR Department the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT Department at school.
- Any online communications must not either knowingly or recklessly: ·

    - place a child or young person at risk of harm, or cause actual harm,
    - bring Spanish School into disrepute,
    - breach confidentiality,
    - breach copyright.
    - breach data protection legislation,
    - be considered discriminatory against, or bullying or harassment of, any individual, for example: making offensive or derogatory comments relating to sex, gender reassignment, race, nationality, disability, sexual orientation, religion or belief or age.
    - use social media to bully another individual,
    - post links to or endorsing material which is discriminatory or offensive.

- School students should not be added as social network 'friends' or contacted through social media.
- Any digital communication between staff and students or parents must be professional in tone and content. Under no circumstances may staff contact a student or parent using their or any other personal email address.
- The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Students

- The school network is protected via a strong anti-virus and firewall protection. Most spam emails and certain attachments are blocked automatically by the email system. Certain websites are automatically blocked by the school's filtering system.
- The school expects students to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be deemed inappropriate or offensive, or likely to cause embarrassment to others.
- Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the Safeguard Committee.
- Students must report any accidental access to inappropriate materials directly to the school IT Department.
- Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on their file and will be dealt with under the school's Behavior Management Policy.
- Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

11. Data Protection

The Spanish School establishes clear expectations for the secure and responsible use of every device connected to our information systems. A computer is issued to a staff member only after the relevant department manager has granted formal authorisation, and it must be surrendered when the employee's contract ends, the individual leaves the school, or the manager requests its return. Once allocated, the user is expected to protect both the physical hardware and the data stored on it: each device is encrypted, covered by remote-wipe capability, and configured to create immediate, continuous backups to the user's Google Drive account.

Digital Data Integrity, Management and Data Safeguarding

- Student/Staff related data must not be deleted from any system either local or in the cloud.
- Student/Staff data must not be shared with outsiders in any form unless the request is from a competent authority for legal proceedings. In such cases, written request from such competent authorities needs to be submitted in official channel.
- Data must not be uploaded to any other web instances other than The Spanish School and ADEK approved sites/portal.
- All data maintained by staffs through joint or individual research/efforts are the intellectual property of the Spanish school and hence the sole ownership rests with the Spanish School.
- Staff when leaving the Spanish School MUST handover the same to IT Department.

Data Storage and Processing

The Spanish School maintains a disciplined backup regimen that fully aligns with the ADEK School Records Policy for both frequency and retention. All critical data—academic records, administrative files, software

images, and network-device configurations—is backed up according to a documented schedule that specifies trimestral full snapshots. When data resides on on-premises servers, each backup copy is encrypted and vaulted to a secure, offline location that is physically and logically separate from the production network, eliminating the risk of simultaneous compromise in the event of ransomware or hardware failure.

For systems that leverage external cloud services, automatic synchronisation ensures that data is continuously mirrored to the school's approved cloud repositories (Google Drive and oneDrive). Integrity checks verify that every transfer completes successfully, and quarterly restoration tests confirm the data can be recovered. By storing at least one backup set off-site and another in the cloud, the school guarantees that vital information remains protected, compliant, and readily restorable under any circumstances.

Staff can back up important Data in the PC with OneDrive and Google Drive folders, so that it is protected and can be recovered in the event of a data failure. No personal data of staff or students should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorized use or suspected misuse of IT must be immediately reported to the IT Department.

12. Safe Use of External Learning Applications

To protect student data and maintain uniform security standards across all third-party educational tools, The Spanish School requires every approved external application to integrate with the school's Google Workspace Single Sign-On (SSO) service. By authenticating through Google SSO, students and staff access external platforms with their existing school credentials; no separate passwords are created, stored, or shared with vendors, thereby reducing the risk of credential theft or reuse.

Before any new application is introduced, the IT Department conducts a security and data-privacy assessment to verify that the vendor supports SAML/OAuth-based SSO, encrypts data in transit and at rest, and complies with UAE data-protection regulations and ADEK guidelines. Applications that cannot meet these requirements are rejected or confined to pilot use under additional safeguards.

Once authorised, each application is provisioned centrally in the Google Admin console, ensuring that user-access rights match classroom enrolments and that off-boarding automatically revokes access when a student graduates or a staff member leaves. Login attempts are protected by the same multi-factor authentication policies and monitoring that safeguard core school systems, and usage logs feed into the school's security-information and event-management platform for anomaly detection.

13. Secure Software Development

Whether developed in-house tools or procure third-party applications, the school requires adherence to OWASP secure-coding principles, including input validation, least-privilege design, and encryption of data in transit and at rest. Source code for internal projects is stored in a private, access-controlled repository; static and dynamic application-security tests run automatically in the CI/CD pipeline. Purchased software must pass a security questionnaire that assesses vendor patch cadence, vulnerability-disclosure processes, and compliance with UAE data-protection law.

14. System Maintenance

The Spanish School follows a structured preventive-maintenance programme to keep all digital and security infrastructure in peak operating condition. Core IT and audiovisual (AV) systems undergo a comprehensive Preventive Maintenance (PPM) service once each academic year, during which technicians inspect hardware components, apply firmware and driver updates, verify backup integrity, and test fail-over procedures.

In addition, CCTV cameras and their recording appliances are serviced on a quarterly PPM cycle that includes lens cleaning, focus and angle verification, storage-capacity checks, and firmware upgrades to ensure continuous, high-quality coverage of critical areas.

Beyond these scheduled visits, the IT Department maintains a monthly patch-management routine for operating systems, network devices, and security appliances; antivirus definitions are refreshed several times per day, and vulnerability scans run after each major update. Automated monitoring tools track disk health, certificate expiry, and network performance in real time, generating alerts that prompt immediate corrective action.

15. Cloud Security

All cloud services, Google Workspace, Microsoft 365, Apple and Securly, are required to process data solely within approved jurisdictions. Resources are configured according to CIS Benchmarks: multi-factor authentication, role-based access control, and customer-managed encryption keys are mandatory. Continuous Cloud-SaaS Security Posture Management—via Google Security Command Center and Microsoft Defender for Cloud Apps—scans for misconfigurations, risky OAuth grants, and anomalous data sharing, alerting the IT team for immediate remediation.

16. Collaboration Security

Communication channels such as Google Meet, Microsoft Teams, and approved Zoom accounts are locked to the school domain by default, with lobby controls activated to block unauthorised participants. Chats are retained for auditing, and file-sharing links expire automatically after 30 days unless extended by a teacher. End-to-end encryption is enabled where supported, and screen-sharing rights are limited to

session hosts. Staff are trained each term on safeguarding etiquette—verifying guest identities, muting inappropriate content, and terminating sessions if misconduct occurs.

17. Virtual Interactiones

Any live virtual session that brings an external guest—such as an author, expert speaker, university representative, or performer—into contact with students must be written parental consentent obtained through the Parent Portal or a signed permission form, clearly stating the date, time, purpose, and platform to be used. No student may participate without this consent.

An event request should be submited to ADEK in accordance with the ADEK School Extracurricular Activities and Events Policy and the ADEK School Student Protection Policy. Approval must be secured and documented before any invitations or meeting links are distributed.

All virtual interactions must be hosted on a school-approved, secure platform (e.g., Microsoft Teams or Google Meet, zoom) using the school's domain accounts, with waiting-room or lobby controls enabled to prevent unauthorised entry. A member of staff—preferably the class teacher—must remain online throughout the session to supervise chat, manage screen-sharing permissions, and intervene if any safeguarding concern arises.

Guest speakers receive a brief code-of-conduct document outlining acceptable language, dress, and interaction protocols, and they are admitted to the virtual room only after staff have validated their identity. Any unexpected behavior, technical issue, or breach of protocol triggers immediate termination of the session and a report to the Coordination Team.

18. Artificial Intelligence

Artificial Intelligence (AI) is a rapidly evolving technology with the potential to revolutionize various aspects of our lives, including education. This policy outlines the guidelines for the acceptable use of AI within our school community, ensuring that it benefits both students and staff while maintaining safety, privacy, and equity.

With regards to AI, The Spanish School is committed to:

- Promoting responsible and ethical use of AI technology within the school environment.
- Ensuring that the integration of AI enhances the educational experience and does not compromise privacy or security.
- Encouraging innovation and creativity in leveraging AI for educational purposes.
- Establishing clear expectations for students, teachers, and staff regarding the use of AI.

Educational Enhancement

AI may be used to enhance educational experiences, such as personalized learning, data analytics for performance improvement, and educational software. The primary goal is to improve learning outcomes and promote academic success.

Privacy and Data Security

- Staff must not share personal data of students with any AI systems. All data collected or generated by AI systems must be stored securely and used solely for educational purposes.
- Personally identifiable information (PII) must be protected according to relevant laws and regulations, such as the Family Educational Rights and Privacy Act (FERPA).

Ethical Considerations

- AI systems must not perpetuate bias or discrimination. Efforts should be made to ensure fairness and equity in their design and use.
- Teachers and students should be educated about the ethical implications of AI technology and encouraged to discuss these issues in the classroom.
- Any use of AI that may infringe upon the dignity or privacy of individuals should be avoided.

Guidelines for Students

- First and foremost, it's essential for students to actively engage with AI as a supplement to their learning, not a substitute. AI can aid in research, data analysis, grammar and spell-checking, and even generating suggestions for improvement. However, it should never replace the critical thinking, creativity, and problem-solving skills that are the core objectives of education.
- Students must also be aware of the ethical considerations surrounding AI usage. This includes citing AI-generated content appropriately, ensuring data privacy and security, and avoiding plagiarism by properly attributing AI-generated assistance in their work.
- Furthermore, students should use AI as a learning opportunity. They should actively seek to understand the algorithms and processes behind AI tools, allowing them to make informed decisions about when and how to utilize AI in their academic pursuits.
- Students are expected to use AI technology responsibly, following the school's code of conduct and adhering to this policy.
- Misuse of AI technology for cheating or academic dishonesty will not be tolerated.

Reporting Concerns

- Students should report any concerns regarding the use of AI technology that may violate this policy to a teacher or school administrator.

Guidelines for Teachers and Staff

- Teachers are encouraged to integrate AI technology into their curriculum when appropriate and beneficial for student learning.
- Training and professional development opportunities will be provided to help teachers effectively use AI in the classroom.

Monitoring and Accountability

- Teachers and staff members using AI systems are responsible for ensuring that they are used in compliance with this policy and applicable laws.
- They should report any technical issues or ethical concerns related to AI technology.

Compliance and Enforcement

Violations of this policy may result in disciplinary action, including but not limited to warnings, loss of access to AI technology, or other appropriate consequences. Decisions will be made on a case-by-case basis.

19. Misuse

- The Spanish School of Abu Dhabi does not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the appropriate authority.
- Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures in particular the Safeguarding Policy.
- The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Anti-Bullying Policy.
- Prompt action will be taken if a member of staff, a student or a parent has a complaint or concern relating to E-Safety. Complaints should be addressed to the school IT Department in the first instance, who will liaise with Senior Leadership, and undertake an investigation where appropriate. Please see the Complaints Policy for further information.
- Incidents of or concerns around E-Safety will be recorded using an Incident Report form and reported to the school's Principal, in accordance with the relevant safety policy of the school.

20. User Compliance

All the terms and conditions mentioned in this policy applicable to all users of internet or devices of the institute.

All the users must agree to abide by this policy by signing the acknowledgement of receipt and understanding of form.

Applies to:

- Stakeholders on campus/off campus
- Faculty and Staff members
- Students
- Administrative Staff (Technical/Non-Technical)
- Higher Authorities and other officers
- Parent/Caregivers
- Visitor/user

Resources:

- Internet Access
- Official websites, web applications
- Official email services
- Data storage
- Documentation Facility (Printers/Scanners)
- Any Other Policy

21. Review and Revision

This policy will be reviewed periodically to ensure its effectiveness and relevance in the ever-changing landscape of technology. Any necessary revisions will be made to reflect new developments and best practices.

Digital Strategy

School landline : 02 31 01 888 School P.O Box: 63797
www.spanishschool.ae info@spanishschool.ae

Digital Strategy

2. DIGITAL STRATEGY AND OVERSIGHT

2.1 Digital Strategy

The Spanish School of Abu Dhabi has developed and implemented a digital strategy aligned with ADEK requirements and Federal Decree Law No. (45) of 2021, establishing a five-year roadmap to ensure the efficient use of technology in teaching, learning, and school administration.

2.1.1 Strategic Direction in Technology

The school is committed to integrating technology into the classroom, ensuring that every student benefits from innovative digital tools. Currently, technology is used to:

- **Enhance learning** through:

  Google Workspace for Education – A cloud-based suite that supports real-time collaborative editing, secure storage and streamlined classroom management. The threaded comment system enables immediate formative feedback and cultivates student self-regulation.

  Microsoft 365 – An integrated platform—including Teams, OneNote and Word—that facilitates teaching, collaboration and content curation. The recent addition of Microsoft Copilot offers generative-AI functions that accelerate lesson planning and differentiated resource creation.

  Apple Education – A comprehensive ecosystem of devices and applications engineered to foster creativity and accessibility. Native apps such as Clips, iMovie and GarageBand encourage project-based learning, while universal accessibility features ensure full inclusion.

  Cambridge – International curricula and assessments aligned with global academic benchmarks. Progress reports enable teachers to calibrate instruction against externally validated standards**.**

  ABT – An assessment platform that measures student progress across multiple domains. Its analytics highlight learning gaps and inform targeted intervention.

MAP NWEA – Adaptive assessments that chart longitudinal academic growth and personalise instruction. Immediate results guide flexible grouping and curriculum differentiation.

ADDITIO – A teacher-management tool that unifies lesson planning, assessment and performance tracking. Built-in rubrics and competency criteria generate automatic report cards, reducing administrative workload.

Canva – A graphic-design platform enabling educators and learners to produce engaging visual materials. The AI-powered Magic Studio allows students to generate illustrations, visual summaries and accessible presentations within seconds.

ProfeDeEle – An online platform providing interactive materials and assessments for teaching Spanish as a Foreign Language (ELE). Its gamified activities and adaptive difficulty levels support differentiated instruction and self-paced practice.

CoPilot, Picsart – AI-enhanced creative tools that simplify advanced image editing and visual expression, facilitating rapid prototyping for STEAM projects.

GeoGebra – Interactive mathematics software delivering dynamic simulations in algebra, geometry, calculus and statistics. Constructions can be exported to OneNote notebooks, encouraging active learning.

Kahoot! – A game-based assessment platform that gauges understanding through live quizzes. Question-level analytics pinpoint misconceptions instantly.

Kid A-Z (Raz-Kids) – A leveled digital library that promotes personalised literacy development. Progress dashboards allow families to track growth at home.

ONMAT – A mathematics environment providing adaptive exercises that adjust continually to student performance.

Anaya – A publisher offering digital textbooks enriched with videos, simulations and auto-graded exercises.

Tekman – A pedagogical methodology combining digital resources with active-learning strategies. Sequenced PBL projects link directly to classroom iPads.

STEAM Future Academy – A programme that supplies hands-on STEAM kits, enabling students to experience the full design-test-iterate cycle.

Edpuzzle – A video-lesson tool that embeds questions and formative checks. Engagement metrics reveal precisely where misunderstanding occurs.

KUTUBEE – An interactive Arabic-and-English reading platform that enhances comprehension with read-aloud support and vocabulary tracking.

Abjadiyat – A gamified application for early Arabic literacy that employs stories, games and adaptive quizzes to sustain motivation.

Alifed.com – A repository of multimedia learning materials across subjects, useful for guided research tasks.

Islamic ISB Assessment – A standards-based evaluation of knowledge in Islamic Studies. Results integrate with ADDITIO to create improvement plans by standard.

Social Studies SSB Assessment – A specialised tool measuring attainment in social-studies content, enabling comparison with national and international averages.

KG ABT – A kindergarten framework that blends assessment with play-based activities to develop fine-motor skills and phonological awareness.

Quran Explorer – A digital environment for interactive Qur'anic study that includes slowed audio playback and bookmarking to support diverse learning needs.

- **Facilitate teaching** with digital screens in every classroom, iPads, and MacBooks for teachers.
- **Optimize administration** with assessment platforms such as NWEA, Cambridge, and Arabic ABT Assessment.

2.1.2 Assistive Technology for Inclusion

The school is committed to ensuring accessibility through Apple's built-in assistive technologies, providing equitable learning opportunities for all students. These tools include:

- **VoiceOver** – A screen reader that provides auditory feedback for visually impaired students.
- **Voice Dictation and Voice Control** – Assist students with motor difficulties by converting speech into text and enabling hands-free navigation.
- **Text-to-Speech and Automatic Captions** – Support students with auditory or language processing challenges through real-time transcription and spoken text.
- **Zoom and Magnifier** – Enhance visibility for students with low vision by enlarging on-screen content.
- **Adaptive Keyboard and Pointer Control** – Customizable settings that facilitate typing and navigation for students with physical disabilities.
- **Live Captions** – Real-time transcription of spoken content to support students with hearing impairments.
- **Speak Selection & Typing Feedback** – Reads selected text aloud and provides auditory feedback while typing, benefiting students with dyslexia or reading difficulties.
- **AssistiveTouch** – Enables students with motor challenges to navigate and control their device more easily.
- **Switch Control** – Allows students with limited mobility to operate their device using external switches.

- **Guided Access** – Restricts device usage to a single app and limits interactions, helping students with attention difficulties stay focused.
- **Background Sounds** – Provides calming background audio to support students with sensory sensitivities.
- **Color Filters & Invert Colors** – Adjusts display settings to assist students with color blindness or visual sensitivities.
- **Siri & Shortcuts** – Voice-activated commands and automation tools that help students with executive function difficulties streamline tasks.

These tools integrate seamlessly across all applications and digital platforms, enhancing accessibility in productivity, learning, and communication environments, regardless of the software or ecosystem used.

2.1.3 Development of Digital Competencies in Students

Students are expected to progressively develop digital skills, including:

- Understanding computing concepts and computational thinking.
- Using digital tools to solve problems and express ideas.
- Basic programming with Scratch, Micro:Bit, or Hydra.
- Digital ethics and cybersecurity, including simulations of online threats.

2.1.4 Digital Infrastructure and Technology Acquisition

The school has the following technological infrastructure:

- **iMacs** in the STEAM Lab and **iPads** distributed across classrooms.
- **MacBooks and iPads** provided to each teacher.
- **A digital screen and iMac** in everyclassroom, ensuring compatibility with laptops, touch devices, and other interactive technologies.

To ensure technological sustainability, a **Device Renewal Plan** will be implemented, including:

- **Replacement of devices every 6-8 years**, based on Apple's lifecycle, with regular performance evaluations to assess functionality and efficiency. Device performance is continuously monitored to ensure optimal operation and timely upgrades when necessary.
- **Periodical updates** for software and applications to maintain compatibility and security.
- **Biannual assessment** of device conditions and network connectivity.

Additionally, secondary students (**Grades 7 & 8**) are issued **individual iPads provided by the school**. These devices remain with the students at all times and may be taken home for continued learning, but they are **returned** to the school at the end of each academic year.

2.1.5 Digital Security

To protect school systems and data, the school has implemented:

- **The Fortinet Firewall & Activity Logging** – The Fortinet firewall continuously monitors and records all network traffic—applications, web access, protocols and IP communications—thus enabling proactive threat mitigation. In accordance with the Data-Protection Policy (8.1 *Data Security and Storage*), access to these logs is restricted to authorised personnel (IT Department and the Digital Well-being Committee), and they are retained under the official retention schedule.

- **Content-Filtering (Securly + Fortinet + JAMF)** – Securly, the Fortinet firewall and JAMF combine to enforce category-based web filtering, application control and policy consistency across all Apple devices. This process satisfies the principles of *Data Minimisation and Accuracy* by preventing exposure to inappropriate content and limiting the collection of personal data.

- **Apple Mobile Device Management (MDM)** – The MDM system applies secure configurations, over-the-air app deployment and automated updates. It reflects the *Authorisation Levels and Access Controls* (Levels 1-5) described in the Data-Protection Plan, ensuring that users can access only data appropriate to their role.

- **Encrypted Cloud Back-ups (Apple, Google, Microsoft)** – Institutional data are backed up automatically with end-to-end encryption. Following the *Data Backup & Recovery Protocol*, regular restoration tests are conducted and strict retention-and-erasure rules applied. In the event of an incident, the *Data Breach Response Plan* mandates notification to the Principal within 24 hours.

2.1.6 Expansion Plan and Digital Future

Over the next five years, the school aims to incorporate emerging technologies, including:

- **3D printing technology** to foster rapid prototyping, design thinking, and interdisciplinary projects.
- **Virtual Reality (VR) and Augmented Reality (AR)** for immersive experiences.
- **Artificial Intelligence** applied to education.
- **Expansion of technological resources** with the gradual acquisition of more iPads.

A percentage of the annual budget will be allocated to digital infrastructure investment and teacher training.

2.1.7 Teacher Training

The school provides continuous training on digital tools, including:

- **Certifications** in Google for Education and Apple Teacher Training.
- **Quarterly training sessions** on new technologies.
- **Internal workshops** led by technology-specialized teachers.

2.1.8 Awareness of Emerging Technologies

- **Annual technology fair** organization.
- **Creation of a STEAM club** to foster innovation.

2.2 Supervision and Control

The **Digital Well-being Committee** oversees the implementation of the digital strategy and associated policies. The committee consists of:

- **School Principal**
- **Head of Studies**
- **Vice Principal**
- **IT Department**
- **Digital Learning Coordinator**

2.2.1 Development and Review of the Digital Strategy

Each year, the **IT Department**, in collaboration with the **Digital Learning Coordinator** and **IT Technician**, reviews the digital strategy with final approval from the **Head of Studies** and **Principal**.

2.2.2 Annual Evaluation and Monitoring

The committee will conduct an annual review through:

- **Monitoring progress** on learning objectives and technological development.
- **Assessment of digital tools** and platforms used in teaching.
- **Security testing and data recovery procedures.**
- **Review of cybersecurity effectiveness and data protection measures.**

2.2.3 Feedback Collection

Currently, there is no structured feedback collection system regarding the digital strategy. An **annual digital survey** will be implemented for:

- **Teachers, students, and families** to assess their perception of technology use in the school.
- **Reviewing suggestions and proposed improvements.**

2.2.4 Development of New Digital Policies

The committee will update and develop new technological policies in accordance with **ADEK regulations** and advancements in educational technology.

2.2.5 Coordination with ADEK

- The **School Principal** serves as the official contact for digital affairs with ADEK.
- **Annual reports** will be submitted detailing digital infrastructure, security, and staff training to ensure compliance with ADEK standards.
- **Security and performance audits** of digital tools will be conducted.

3. DIGITAL COMPETENCIES

3.1 Student Outcomes

The Spanish School of Abu Dhabi has defined expected digital competencies by educational stage and integrated them into the curriculum. The school provides the necessary **technological infrastructure and resources** to ensure that all students, including those with special educational needs, can achieve these goals, in compliance with ADEK's **School Inclusion Policy**.

3.1.1 Digital Competencies by Educational Stage

- **Early Years (Pre KG - KG2):** Introduction to digital devices and interactive applications.
- **Primary Years 1-2:** Basic digital navigation, creative tools, and online safety.
- **Primary Years 3-4:** Digital research, content creation, and collaborative tools.
- **Primary Years 5-6:** Computational thinking, programming, and cybersecurity.
- **Secondary (Years 7-9):** Digital communication, content creation, and data security.
- **Senior Secondary (Years 10-12):** Advanced digital projects, content evaluation, and online citizenship.

3.1.2 Curriculum Integration

Digital competencies are embedded in the curriculum through:

- **Early Years** – Pupils engage in teacher-guided exploration of tablets and interactive screens, developing foundational hand-eye coordination, fine-motor skills and responsible device handling.

- **Primary Education** – Alongside structured lessons in digital literacy and online research, each class follows a dedicated **STEAM subject block** where students practise basic programming with visual languages such as Scratch Jr or Micro:Bit, laying the groundwork for computational thinking.

- **Secondary Education** – The programme advances to text-based coding, robotics, data analysis and interdisciplinary STEAM challenges that culminate in authentic design projects.

- **Methodology & Assessment** – Across all phases, project-based learning, gamification and cloud-based digital portfolios document growth, promote reflection and deliver timely feedback.

3.1.3 Support Infrastructure

The school maintains a robust, multilayered technology environment that underpins day-to-day teaching and learning:

- A purpose-designed STEAM laboratory is equipped with a full suite of iMac desktop computers, giving learners the processing power and creative tools required for advanced multimedia, coding and design projects.
- A fleet of classroom-ready iPads is distributed across the grade levels, providing students and teachers with flexible, touch-based devices that support individual exploration, quick formative assessment and seamless integration with cloud-based resources.
- Every classroom is fitted with an interactive digital screen and a dedicated teacher workstation, enabling educators to weave rich media, live demonstrations and collaborative tasks seamlessly into regular instruction.
- Staff and students enjoy institution-wide access to an extensive portfolio of educational software—including Google Workspace for Education, STEAM Future Academy, Additio and Cambridge digital resources—which streamlines communication, assessment and curriculum alignment across all subject areas.

3.1.4 Digital Inclusion

The school is committed to fostering an inclusive digital environment where all students have equitable access to technology. This is achieved through the implementation of assistive tools and accessibility features, as detailed in section **2.1.2 Assistive Technology for Inclusion**, which outlines the built-in Apple accessibility tools and their integration across digital platforms.

3.2 Staff Training

3.2.1 Current Training

Teachers receive continuous training in:

- Digital tools and platforms.
- Data security and digital protection strategies.
- Integration of new technologies in education.

3.2.2 Future Training Plan

The school plans to implement a **Professional Digital Development Program**, including:

- Regular training sessions.
- Specialized courses in educational technology.
- Impact assessments to measure training effectiveness.

Framework For The Selection Of External Providers And Products

School landline : 02 31 01 888 School P.O Box: 63797
www.spanishschool.ae info@spanishschool.ae

1. *Purpose*

This framework ensures all external providers and products selected for the Spanish School of Abu Dhabi strictly comply with ADEK guidelines, UAE regulations, and best practices while guaranteeing seamless integration within the school's diverse technological infrastructure, including Apple, Alcatel, HP, Brother, Konica, Canon, Zebra, Hikvision, Fortinet, Dell, Viewsonic displays, Google, Microsoft, Bose, and Toa sound system.

2. *Scope*

This comprehensive framework applies to external vendors providing software, hardware, digital educational solutions, cloud services, and IT-related products tailored specifically to the technological infrastructure of the Spanish School of Abu Dhabi.

3. *Selection Criteria*

3.1. Data Protection and Privacy

- Providers must furnish detailed documentation outlining data collection, usage, processing, storage, and deletion practices.
- Explicit, informed consent procedures must be clearly defined, accessible, and easy to manage, including straightforward consent withdrawal processes.
- Clearly outlined processes for data portability, correction, and deletion must be demonstrated, including user-friendly interfaces.
- Adoption of advanced encryption standards, detailing encryption methodologies used for both data at rest and during transmission.
- Implementation of rigorous pseudonymisation and anonymisation techniques to protect sensitive data.
- Comprehensive, proactive protocols for identifying, managing, and reporting data breaches, including timely notification to all relevant stakeholders.

3.2. Cybersecurity Standards

- Proven compliance with internationally recognized cybersecurity frameworks such as ISO/IEC 27001, including certification or independent audits.
- Demonstrated capability to effectively prevent, detect, and respond to cybersecurity threats, including malware, phishing, ransomware, and unauthorized access attempts.
- Clear compatibility with the school's security infrastructure.

3.3. Technological Integration and Compatibility

- Full compatibility and seamless integration with the existing infrastructure of Apple devices, Alcatel network, Dell computing equipment, Brother, Konica, Canon and HP printing equipment, Viewsonic displays, Google, Microsoft, Hikvision surveillance, and Bose and Toa sound systems.
- Confirmed support and compatibility with current Mobile Device Management (MDM) solutions and other network management tools, if required.
- Commitment to regularly scheduled updates and improvements aligned with technology vendors' update cycles and long-term product support commitments.

3.4. Educational Quality and Relevance

- Thorough alignment with curricular objectives, standards, and educational outcomes specified by the Spanish School of Abu Dhabi, ADEK and The Spanish Ministry of Education, Vocational Training, and Sports.
- Content delivered must be age-appropriate, multilingual, culturally respectful, and enriching for diverse student demographics.
- Demonstrable use of extensive accessibility features across the school's technology landscape to promote inclusive education and support students with additional learning needs effectively.

3.5. Cybersecurity Infrastructure

- Deployment of secure authentication mechanisms, including multi-factor authentication (MFA) across all relevant services and systems.
- Regularly scheduled penetration testing, vulnerability assessments, and continuous security audits with documented remediation processes.
- Secure update and patch management practices to ensure vulnerabilities are quickly identified and resolved.

3.6. Vendor Stability and Reputation

- Comprehensive evaluation of the provider's market reputation, financial stability, and operational history, particularly focusing on educational sector experience.
- Collection and review of positive customer references and testimonials, especially from UAE-based educational institutions.
- Evidence of reliable, responsive, and consistent post-sales support, demonstrated by historical performance data and customer feedback.

3.7. Service Delivery and Support

- Clearly defined Service Level Agreements (SLAs) outlining specific metrics for service reliability, including uptime guarantees, technical support response times, and problem resolution timeframes.
- Availability of comprehensive training programs, technical support services, online resources, and dedicated support teams for staff and students.
- Documented business continuity, disaster recovery, data backup procedures, and evidence of successful periodic testing and validation.

3.8. Cost Efficiency and Sustainability

- Detailed, transparent cost-benefit analyses encompassing all expenses, including initial setup, ongoing maintenance, licensing fees, software upgrades, and lifecycle management.
- Demonstrable long-term vendor commitments to product sustainability, ongoing software updates, enhancements, and continued compatibility with the evolving technological ecosystem.

3.9. Environmental Sustainability

- Clear demonstration of provider commitment to environmentally sustainable practices, including environmentally friendly packaging, responsible recycling initiatives, and energy-efficient technology solutions.
- Availability of sustainability certifications or compliance with international environmental standards.

3.10. Innovation and Development

- Demonstrable commitment to ongoing technological innovation, research, and continuous product improvement, particularly in educational technology.
- Clear evidence of adaptability and responsiveness to emerging technological trends, specifically within the school's diverse technology ecosystem.

4. Evaluation and Approval Process

- Submission of detailed compliance, technical, and product specifications documentation by potential providers.
- Comprehensive technical and cybersecurity evaluations.
- Detailed educational content evaluation by relevant academic departments.
- Rigorous risk assessments focusing on data protection and cybersecurity.
- Final review, comprehensive evaluation, and recommendations by the Safeguarding Committee.
- Formal and documented approval by the School Principal.

5. ***Contractual Obligations***

- Detailed contractual clauses explicitly addressing data privacy, cybersecurity measures, and vendor accountability.
- Inclusion of strict confidentiality and non-disclosure agreements prohibiting unauthorized sharing or misuse of school data.
- Defined and enforceable procedures and timelines for immediate notification, response, and resolution of data breaches or cybersecurity incidents.

6. ***Compliance Monitoring***

- Annual comprehensive audits, continuous compliance monitoring, and periodic reviews of all external vendors.
- Regular cybersecurity and data privacy assessments conducted to ensure ongoing vendor compliance.

7. ***Policy Review***

- Annual review and updates of this framework, integrating technological advancements, regulatory changes, and feedback from the school community to ensure continuous effectiveness and compliance.

Data Protection Policy

School landline : 02 31 01 888 School P.O Box: 63797
www.spanishschool.ae info@spanishschool.ae

1. Introduction

At The Spanish School of Abu Dhabi we believe that the protection of all data is in the best interest of staff and students. The School collects and uses personal information about staff, students, parents and other individuals who come into contact with the School. This information is gathered in order to enable the provision of education and other associated functions. In addition, the School may be required by law to collect, use and share certain information.

The School issues a Privacy Notice to all students/parents, this summarises the information held on pupils, why it is held and the other organisations to whom it may be passed on to.

2. Aims

This policy sets out how the School deals with personal information correctly and securely and in accordance with the expectation of confidentiality.

This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.

All School staff involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

3. Legislation and guidance

This policy complies with Federal Law No. 45 and the ADEK regulations on data protection. It ensures adherence to relevant guidelines concerning the use of personal data, biometric data, and surveillance systems within educational institutions.

4. Roles and Responsabilities

This policy applies to all staff employed by our School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5. Digital well-being Committee

The Spanish School of Abu Dhabi has a designated digital well-being committe who oversee policy and practice relating to all elements of online safety and digital platforms:

- **Principal**: To oversee the safety and security of online systems and digital platforms, and to make final decisions regarding related policies and practices.

- **Head of Studies:** To oversee the implementation and monitoring of educational technology and manage the handling of policy breaches throughout the school.

- **IT Department**: To oversee Whole School Digital Infrastructure and associated policies.

All staff members must ensure they:

- Collect, store, and process personal data according to the school's data protection policy.
- Promptly inform the school administration whenever their own personal information changes, such as updates to their address or contact details.
- Staff should contact the IT department in any of the following situations:
    - If they have questions or require clarification about this data protection policy, including procedures for secure storage, lawful retention, or correct handling of personal data.
    - If they are concerned or aware of potential breaches or non-compliance with the policy.
    - If they are uncertain whether they have a valid legal basis to use or process personal data in a particular context.
    - If they require support to obtain consent, draft privacy notices, respond to data subject requests, or manage transfers of personal data outside the UAE.
    - Immediately upon discovering or suspecting a data breach or security incident involving personal data.
    - Before beginning any new activities or projects that could affect the privacy rights of individuals.
    - When needing assistance in handling or reviewing contracts, particularly those involving the sharing or handling of personal data with external third parties.

All members of the school community are expected to positively and responsibly use technology and adhere to data protection guidelines established by the school.

6. *Data Protection Principles*

The following principles that must be adhered to at all times:

- Personal data must be processed fairly, lawfully, and transparently in compliance with regulations.
- Personal data must be collected only for specified, explicit, and legitimate purposes.
- Personal data must be adequate, relevant, and not excessive for its intended purpose.
- Personal data must be accurate and kept up to date when necessary.

- Personal data must not be retained for longer than necessary and must be securely deleted or anonymized when no longer required.
- Personal data must be processed in accordance with the rights of data subjects and international best practices.
- Personal data must be secured against unauthorized access, processing, loss, destruction, or damage through appropriate security measures.
- Access to personal data is restricted to individuals who:
    - Have proper authorization.
    - Have a legitimate official requirement to access the data.
- Individuals handling personal data must be aware of and comply with this policy and relevant data protection laws.
- Data breaches can have serious consequences, including harm to individuals and institutions, reputational damage, and disciplinary action.
- Legal Compliance in the UAE:
    - Articles 378 and 379 of the UAE Penal Code impose imprisonment and fines for breaches of privacy.
    - Federal Law No. 5 of 2012 on Combatting Cybercrimes criminalizes unauthorized disclosure of electronically obtained information.
    - Article 22 of the same law holds individuals liable for unauthorized use of IT resources to disclose confidential information obtained through work.

7. Collecting Personal Data

1. Lawfulness, Fairness, and Transparency

The Spanish School of Abu Dhabi processes personal data strictly adhering to established legal grounds, ensuring fairness and transparency by clearly informing individuals about the purpose, methods, and necessity of data collection and processing.

Personal data will only be processed under one or more of the following lawful bases:

- Contractual Obligation: Data processing required to fulfill a contractual agreement with the individual, or necessary preliminary steps requested by the individual before a contract is finalized.
- Legal Obligation: Data processing mandated by UAE law, regulations, or statutory obligations to which the school is subject.
- Vital Interests: Processing necessary to protect an individual's life, health, or safety in urgent situations.

- Public Task: Processing essential for the school's performance of public duties, such as providing education and ensuring student safety, as regulated by educational authorities like ADEK.
- Legitimate Interests: Processing pursued for legitimate interests of the school or third parties, provided these interests do not override the rights and freedoms of affected individuals.
- Consent: Explicit and informed consent given freely by the individual or, in the case of minors, their parent/guardian, allowing the school to process their personal data.

For processing special categories of personal data, which include sensitive information such as health and biometric data, the school strictly adheres to the special conditions outlined in UAE data protection legislation, including explicit consent and higher security measures.

When offering online services such as classroom applications, parental consent will be explicitly obtained for all students, except when using online counselling or preventive services lawfully exempt from this requirement.

2. Limitation, Minimisation, and Accuracy

Personal data will only be collected for explicitly stated and legitimate purposes, explained clearly to individuals at the initial collection stage.

If personal data needs to be processed for purposes other than initially declared, the individuals will be informed in advance, and additional consent will be obtained when required.

Staff must only handle personal data strictly necessary to their job role. Data no longer required for its initial purpose must be securely deleted or fully anonymized.

3. Individual Consent Requirements and Procedures

The school adheres strictly to the following consent requirements and procedures:

- Consent obtained from individuals must always be:
  - Freely given: Without any form of pressure or coercion.
  - Specific: Clearly indicating the exact purposes for which consent is sought.
  - Informed: Individuals are provided all necessary information regarding the data collection, storage, processing, and sharing details.
  - Unambiguous: Explicit, clearly stated, and verifiable.
- Individuals retain the right to withdraw their consent at any time. Upon withdrawal, the school will cease further processing and take necessary steps to manage previously collected data in compliance with UAE law and policy standards.

4. Conditions for Sharing Personal Data

Personal data may be shared under controlled conditions and strict guidelines, including:

- Safety and Welfare: Where the safety of students, staff, or parents/guardians is at stake, sharing data is permitted to protect these interests.
- External Contractors and Vendors: Personal data may be shared with external contractors and vendors providing necessary services (e.g., IT or educational services). In these cases, the school ensures:
    - Contractors comply fully with UAE data protection regulations.
    - Inclusion of robust non-disclosure agreements (NDAs) in contracts, explicitly prohibiting the sharing of personal data within or outside the UAE without explicit consent from ADEK.
    - Clearly defined and documented data-sharing agreements outlining permissible data use, security obligations, and accountability measures.
- Sharing Data with ADEK: The school is legally required and authorized to share accurate, current, and relevant data with ADEK upon request. This data sharing is compliant with:
    - Federal Decree Law No. (18) of 2020 concerning Private Education (and its amendments).
    - Law No. (9) of 2018 on the Establishment of ADEK.
    - ADEK's specific terms and conditions, and their stated data privacy policy governing data collection, usage, and disclosure.
- Parent and Guardian Notification: Parents and guardians are clearly informed of the school's legal obligations to share student data with ADEK, ensuring full transparency and awareness within the school community.
- Law Enforcement and Government Bodies: Data will also be shared with law enforcement and relevant governmental bodies as mandated by law, particularly for crime prevention, legal proceedings, or safeguarding responsibilities.
- Emergencies: Data sharing with emergency services or local authorities is permitted during situations affecting the health, safety, or wellbeing of any member of the school community.
- International Transfers: Personal data transferred outside the UAE is only done under stringent legal safeguards compliant with applicable UAE data protection regulations, ensuring continued security and confidentiality.

5. Specification of Data Collected

In compliance with Federal Decree Law No. (45) of 2021, the following categories of personal data are collected and processed:

1. Student data

- Full name, date of birth, and gender
- Academic records, grades, and attendance
- Behavior reports and disciplinary records
- Health information (if required for school services)
- Student file (includes joining details, health records, UAE residence status, Parent's occupation details, educational background (previous school details, emergency contact details), and withdrawal applications.
- co-scholastic records
- Documents and recordings for marketing and Promotion, survey responses, such as parent satisfaction score, school feedback and school rating criteria, etc.

2. Staff and Teacher Data:

- Full name, contact details, and identification documents
- Employment qualifications and certifications
- Payroll and banking information
- Performance evaluations and training records.
- Medical Documents
- Staff records (includes residence status, work experience details, previous employee details, educational background, health records, emergency contact details, visa, contract letters, promotion letters, leave applications, warning letters, incident reports, exit interviews, terminations/resignations)

3. Parent and Guardian Data

- Name, contact details, and relationship to the student
- Communication records with the school
- Payment and billing information.

4. IT and Digital Access Data

- User credentials: (email, usernames, and details) for Google, Microsoft and Apple services
- Device information: (IP addresses, MAC addresses, and login history, Location)
- Network activity logs: (internet usage, access to school platforms, and security logs)
- Biometric data: (if applicable, for security and authentication purposes)

5. Security and Safeguarding Data

- CCTV footage within school premises
- Access control logs (entry and exit records)
- Incident reports and safety monitoring data

All collected data is processed in accordance with data protection regulations, ensuring confidentiality, security, and limited access based on necessity.

8. Subject Access Requests and Individual Data Rights

Individuals have the right to submit a Subject Access Request (SAR) to access personal information held about them by The Spanish School of Abu Dhabi. This right includes:

- Confirmation that their personal data is being processed.
- Access to a copy of their personal data.
- Details about the purposes of the data processing.
- Information on the categories of personal data being processed.
- Information about any third parties with whom the data has been, or will be, shared.
- Information regarding how long the data will be stored, or criteria used to determine the retention period.
- The source of the data, if not directly obtained from the individual.
- Information on any automated decision-making applied, including potential consequences for the individual.

All SARs must be made in writing (email or letter) directly to the school's IT Department. Requests must clearly include:

- Full name of the individual.
- Contact number and email address.
- Details of the specific information requested.

If staff members receive a SAR, they must forward it immediately to the IT Department.

1. Subject Access Requests Involving Children

Personal data related to students belongs primarily to the student, rather than parents or guardians. Parents or guardians may submit a SAR for their child's data only if:

- The child has given explicit consent, or

- The child is considered unable to understand their own data rights.

Typically, students aged 12 and above are presumed to understand their rights, and requests from parents or guardians may require explicit consent from the student. Decisions will be made on a case-by-case basis, considering the maturity and understanding of the individual student.

2. Responding to Subject Access Requests

Upon receiving a SAR, the school will:

- Verify the requester's identity (typically requiring two forms of identification).
- Contact the requester if clarification is needed.
- Respond without delay and within one month of receipt.
- Provide requested information free of charge.
- Inform the requester within one month if additional processing time (up to three months) is required, clearly explaining the reason.

The school may refuse a SAR or charge a reasonable fee if the request is repetitive, unfounded, or excessive. If a request is refused, the reasons will be clearly communicated, and the requester informed of their right to lodge a complaint with the Principal.

The school may withhold certain data if disclosure:

- Risks causing significant harm to the physical or mental health of any individual.
- Could reveal that a child is at risk of abuse where disclosure would not be in the child's best interest.
- Relates to adoption or parental order records.
- Is confidential within court proceedings involving the child.

3. Other Individual Data Protection Rights

Individuals associated with the school have the right to:

- Withdraw consent to data processing at any time.
- Request rectification, erasure, or restriction of data processing (where applicable).
- Object to data processing (under certain circumstances).
- Prevent personal data usage for direct marketing.
- Challenge data processing justified by public interest.

- Request copies of agreements governing international transfers of personal data.
- Object to automated decision-making and profiling.
- Be notified promptly in case of a data breach affecting their data.
- Lodge complaints regarding data handling directly with the Principal.
- Request data portability—transfer their data in a structured, machine-readable format to another entity (under specific circumstances).

Requests to exercise these rights must be directed to the IT Department. Staff receiving such requests must forward them promptly to the IT Department.

4. Parental Requests for Educational Records

Parents or guardians wishing to view their child's educational record must submit a written request to the school.

5. CCTV Surveillance

The school utilizes CCTV cameras throughout the school campus for safety, security, and safeguarding purposes. Footage is accessible only by authorized Senior Leadership Team (SLT) members for investigative purposes. Enquiries regarding CCTV usage should be directed to the Principal.

6. Photographs and Video Recordings

The school captures photographs and videos of students for educational, promotional, and communication purposes. Upon enrollment, explicit written consent is obtained from parents/guardians.

Potential uses include:

- Internal displays, notice boards, newsletters, and handbooks.
- External promotional materials, school publications, and media outreach.
- Online platforms such as the school's website and social media channels.

Consent may be refused or withdrawn at any time. Upon withdrawal, images or videos will be promptly removed from future use. Photos/videos taken by parents or guardians for personal use are permitted, provided they avoid capturing other students without explicit permission.

7. Data Protection by Design and Default

The school integrates robust data protection practices by:

- Conducting Data Protection Impact Assessments (DPIAs) for new technologies and processes involving significant risks to data privacy.
- Providing regular data protection training for all staff, maintaining attendance records.
- Regularly reviewing and auditing data processing practices to ensure ongoing compliance.
- Maintaining detailed records of data processing activities, clearly documenting the nature, purposes, and security measures related to the data held.

8. Data Security and Storage

Personal data is safeguarded against unauthorized access, accidental loss, or destruction through the following measures:

- Secure storage (locked facilities for physical records, encrypted storage for electronic data).
- Password protection and regular password updates for all digital devices.
- Secure and encrypted portable devices and removable media.
- Ensuring third-party service providers adhere strictly to data protection requirements.
- Expecting staff who store personal data on personal devices to follow the same security protocols as for school-owned devices.

9. Disposal of Personal Data

The school securely disposes of personal data no longer required or deemed inaccurate by:

- Shredding or securely incinerating paper records.
- Securely overwriting or deleting electronic files.
- Ensuring third-party disposal services provide adequate guarantees of compliance with data protection standards..

10. Training and Monitoring

All staff and governors receive ongoing data protection training. This policy will be reviewed annually by the IT Department, with updates reflecting changes in legislation or school procedures.

11. Equality Impact Statement

The school commits to ensuring this policy does not directly or indirectly discriminate against any individual. Regular evaluations will monitor the impact of this policy on promoting equality and cohesion within the school community.

9. *Data Protection Plan*

The Spanish School of Abu Dhabi is fully committed to safeguarding all organizational and personal data. The plan details clear protocols around data classification, authorization levels, cybersecurity measures, backup procedures, data-sharing protocols, and enforcement measures.

1. Data Classification and Management

All school data is periodically reviewed and classified according to sensitivity, usage, value, and criticality. Data classification guides how the school secures and protects each type of information.

The following data classification categories apply:

- **Restricted Data:** Highly sensitive information requiring stringent security measures due to regulatory, legal, or contractual obligations. Access to restricted data is strictly limited to authorized personnel and approved business partners. Unauthorized disclosure of restricted data could lead to significant legal consequences, severe reputational damage, or identity theft. All breaches of restricted data must be promptly reported and managed in line with legal obligations.

- **Confidential Data:** Important, sensitive information owned by or entrusted to the school. Unauthorized disclosure of confidential data can adversely impact school operations or reputation. This information is accessible only to authorized staff, approved contractors, or business partners who have signed appropriate confidentiality or non-disclosure agreements.

- **Public Data:** Information officially approved for release to the general public, internally and externally accessible. Disclosure of public data does not present any risk or damage to the school or individuals involved.

- **Personally Identifiable Information (PII):** Information capable of identifying an individual, such as full names, identity numbers, dates of birth, contact information, biometric data, financial details, or medical records. Handling of PII follows stringent security and privacy guidelines.

- **Protected Health Information (PHI):** Health-related data requiring rigorous protections to ensure privacy and regulatory compliance. This includes medical history, health conditions, or any related identifiable data.

By default, all data shall be treated as Restricted unless explicitly classified otherwise.

2. Authorization Levels and Access Controls

Data access at the Spanish School of Abu Dhabi is governed by clearly defined authorization levels:

- **Level 1 (General Access):** Basic, read-only access to public information available to all school community members and external stakeholders.
- **Level 2 (Staff Access):** Access granted to teaching and administrative staff for relevant confidential documents and operational data necessary to perform their duties.
- **Level 3 (Managerial Access):** Extended access for departmental heads and senior administrators to confidential operational, financial, and administrative records.
- **Level 4 (IT and Security Access):** Specialized access reserved for IT administrators and security personnel, including full access to cybersecurity infrastructure and sensitive organizational systems.
- **Level 5 (Executive Access):** Comprehensive access granted exclusively to the Principal, IT Manager, and authorized senior executives, encompassing all data categories, including highly confidential legal, financial, and sensitive personal information.

All staff receive regular training on data protection requirements, and elevated access requests must be formally documented and approved by the IT Department.

3. Cybersecurity and Threat Prevention

The Spanish School of Abu Dhabi employs advanced cybersecurity protocols, including:

- Robust firewall configurations, secure data encryption methods, and multi-factor authentication across systems.
- Regular vulnerability assessments and cybersecurity audits to detect and mitigate potential security threats proactively.
- Comprehensive password policies, secure Wi-Fi networks, and restricted remote access policies.
- An established incident response plan to ensure swift action against cybersecurity incidents, minimizing impact and facilitating rapid recovery.

4. Data Backup and Recovery

The school data backup procedures include:

- Regular, automated, encrypted backups of all critical data, stored securely on-site and through cloud solutions (Google Drive, Microsoft OneDrive, and Apple iCloud).
- Routine backup tests and restoration drills to verify data integrity and reliability.
- Immediate and clear procedures for data restoration in case of data loss, corruption, or breaches, ensuring minimal disruption to school operations.

5. Compliance and Continuous Monitoring

The Spanish School of Abu Dhabi ensures ongoing data protection compliance through:

- Regular internal policy reviews and updates, aligning with evolving legislation and ADEK guidelines.
- Annual internal audits and risk assessments evaluating data security effectiveness and identifying potential improvements.
- Continuous training sessions provided to all staff members and stakeholders, reinforcing responsibilities regarding data security and confidentiality.

6. Enforcement and Violations of Data Protection Policy

Breaches of data protection procedures are regarded seriously. Each staff member signs a non-disclosure agreement (NDA) ensuring confidentiality, pledging not to disclose any information without explicit authorization.
Staff found in violation of the NDA or data protection policies may face disciplinary actions, including termination of employment, and could also be liable to provide compensation for any damages caused to the school.

7. Remote Access and Data Handling

Personnel remotely accessing restricted or confidential data must not copy, transfer, or store such data on local or removable storage unless explicitly authorized for specific, documented purposes. Data transferred through external networks or unsecured channels must always be encrypted.

8. Data Breach Response and Reporting

In the unlikely event of a data breach, the following protocol is enacted immediately:

- Immediate reporting of suspected or confirmed breaches to IT Department.
- Investigation by the IT Department to assess the nature, scale, and impact of the breach.
- Notification to the Principal and relevant authorities within 24 hours if severe implications are identified.
- Immediate actions to contain, minimize, and mitigate the damage, with affected parties informed as soon as possible.
- Documentation of the breach event, response actions, and follow-up reviews stored securely for accountability and future prevention.

10. Sanctions on violating the policy

	Low severity		Medium Severity		High Severity	
Incident Details	Reporting to Immediate Supervisor	First Action Plan - Verbal Warning	Second Level Plan- written warning letter from Leadership	Suspension from job for 2 days	If repeating, Suspension from job until further notice	Reporting to External Agency/ Police
Irresponsible while handling print outs of confidential documents	•	•	•			
Making unofficial copies without consent	•			•	•	
Disclosing personal/sensitive data of any other person	•		•		•	
Back up of confidential data without consent	•		•		•	
Sharing the confidential data with the third party for self benefit	•				•	•

Responsible Usage Policy

School landline : 02 31 01 888 School P.O Box: 63797
www.spanishschool.ae info@spanishschool.ae

1. Introduction

The Spanish School of Abu Dhabi makes a variety of communications and information technologies available to students and staff through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the school by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the school, its students and its employees. This Acceptable Use policy is intended to minimize the likelihood of such harm by educating school users and setting standards which will serve to protect the school. The school firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

2. Aim

The aim of the Responsible use policy is to ensure that all Students, Staff and Parents are aware of the risks and hazards of internet usage and use it sensibly and safely for the purpose of information sharing and improved learning. All students and staff should know about the Responsible use of technologies. All students and staff should be free of any fear of cyber bullying by anyone known or unknown, should be able to recognize cyber bullying and be fully equipped to be able to deal with it effectively as well as are fully competent in surfing internet safely.

3. Legal underpinning of the Policy

School is dedicated to complying with ADEK guidelines and the UAE Federal law no.2/2006 dated 3/1/2006: 'The Prevention of Information Technology Crimes' which provides clear guidelines regarding what is permissible and what is punishable in the usage of cyber space. School also assumes the responsibility of raising awareness against cybercrimes especially against children and training students, parents and staff to be smart digital citizens.

The UAE Student Conduct Disciplinary Bylaw and the Federal Decree-Law no. (5) outline that deliberately creating, transferring and publishing photos and comments on social media that undoubtedly shows defamation of individuals or staff members, or School Leadership of character, dignity and integrity are breaking the law.

This policy describes the responsible use of digital technology. It is designed to minimize the risk to students, protect employees and the school from litigation as well as maintain levels of professional standings.

The policy is designed to ensure the safe and responsible use of electronic devices by all users, both on the school premises and elsewhere in which the school is represented. In order to use the school's digital resources, they must follow the guidelines set forth in this this policy. The rules written in this agreement are not all inclusive.

The school reserves the right to change this agreement as when it deems it necessary to do so. It is a general agreement that all facilities (hardware, software, Internet, etc.) are to be used in a responsible, ethical, and legal manner, in and out of school.

By using any digital resources, whether owned personally or by the school, users acknowledge their understanding of the Electronic Devices / Digital Resources / BYOD Agreement as a condition of using such devices and the Internet.

The school provides some electronic devices and services to promote educational excellence. The school has a responsibility to maintain the integrity, operation, and availability of its electronic systems for access and use. Whilst on site, access to the school network and the Internet should be considered a privilege, not a right, and can be suspended immediately, without notice. Access on site is available only for educational and administrative purposes.

Digital resources are to be used in accordance with this Policy and all users will be required to comply with its regulations. The guidelines provided in this policy are intended to help users understand appropriate use. The school may restrict, suspend, or terminate any user's access to the school's computer systems upon violation of this Policy. This policy applies to all digital resources, not only the computers, devices and equipment provided in the school's IT Department, but also the personal devices staff/students bring to school.

The purpose of the 'Electronic Devices / Digital Resources / BYOD acceptable Use' Agreement is to ensure that all students use technology in school, at home and elsewhere, effectively, safely and responsibly, to facilitate learning on a 24/7 basis, and to help ensure that they develop the attributes of competent digital citizens.

4. Principles of Acceptable and Safe Internet Use

- The school places ownership on all internet data that is produced, received or transmitted. This data can be revealed for appropriate requirement such as legal matters or investigative matters.
- All electronic paraphernalia both hardware and software, expertise and services involved in the usage of internet belong to the School and the School has the right to access and monitor all data and internet interchange.
- All emails sent through the school email system might be monitored to discourage use of offensive mails.
- All sites and downloads may be monitored or blocked by school if the school considers them.
- unsuitable or they are thought to be damaging to the School, Staff and Students.
- Unauthorized installation of software is not permissible at all.
- Usage of storage media which is not scanned prior to usage is strictly prohibited in order to limit spread of Viruses and other malicious software.

5. Acceptable uses of the school's internet systems for Students are:

- Using the web browsers for educational purposes of research and information gathering from various websites and databases.
- Using the internet for sharing documents and assignments promoting collaborative work.
- Keeping the allocated personal username and password confidential, not sharing with anyone.
- Not trying to access and change any other person's username, password, files or data.
- Sharing emails only with people known to oneself and approved by parents or teachers.
- Using internet to do online tests or tasks approved or advised by the teachers.
- Studying syllabus content online and performing tasks pertaining to it with teachers' authorization.
- Doing projects or presentations for the lessons.
- Preparing circulars, invitations, information pamphlets for community service or other school activities with the teachers' approval.
- Accessing examination sites for practice papers and answer schemes.
- Responsibly accessing social websites for educational purposes only under teachers' guidance.
- Always using appropriate language in all digital communications through emails, socialwebsites, blogs or messages
- Taking good care of all digital devices in use

6. Acceptable uses of the School's internet systems for Staff are:

- Being committed to a responsible and effective use of the internet
- Using Internet only for School related purposes and not for personal matters
- Participating in all activities that help enhance and improve the professional aspect of any employee would be acceptable including online research and training
- Ensuring there is no unauthorized use of internet by anyone in the School
- Using all available online teaching resources in the teaching and learning activities involving research and collaboration with other professionals in the educational field
- Enhancing the IT skills and competencies of students to improve their learning
- Promoting the use of the Internet to support career counselling and investigating options forhigher education most suited for individual students' interest
- Supporting students' personal and social development through focused lessons with cross curricular links, cross country collaborative projects, e-learning and real life experiences
- Sharing good teaching practices involving advanced IT skills

7. Prohibited Uses of the School's Internet System for all users:

- Using emails to threaten or harass other people

- Sending or posting disturbing images on the internet
- Using internet to commit any kind of piracy like music, film or software □ Sharing passwords or using and distributing passwords of others
- Violating the copyright law with respect to downloading or copying electronic files for personalusage
- Sharing School's confidential matters or information without authorization
- Compromising the security of the electronic system of the School by introducing malicious software
- Using the internet to promote personal business □ Visiting unauthorized websites
- Distributing any information which is incorrect, offensive or slanderous □ Using threatening and inappropriate language in communications
- Damaging the hardware or software
- Deliberately causing harm to someone's work or program
- Involving in cyber bullyingIndulging in plagiarism
- Accessing pornographic sites or sites that promote hatred, discrimination, racism □ Disclosing personal information about oneself without authorization
- Visiting social websites without authorization
- Using someone else's information, images of work without permission

8. *Acceptable uses of the school's technology systems – Students*

- School devices are the sole property of the school, and all users will follow this policy
- School devices are intended for educational use only
- Any school device can be used only after the respective teacher has permitted use
- Music and internet games on school devices are allowed at the discretion of the teacher
- Games, apps, software, screen saver, backgrounds etc. should not be downloaded on school devices without permission from school IT department
- Do not change any device settings without permission from IT department
- Turn off all devices after you are done working on it
- All devices should be used in a responsible manner
- Do not write or label on school devices
- Any damage to the school devices will lead to disciplinary action by school administration.

9. *Acceptable uses of the school's technology systems – Staff*

- School devices are intended for educational use and not for personal matters
- Do not change any device settings without permission from IT department
- Do not share your username and password with anyone and ensure that you change it at regular intervals
- Do not use the system if the previous user has not logged out. Either log out and use your credentials, or approach the IT department for support
- Do not save personal files or data on school systems
- Do not download or install any program, software or hardware without permission
- Turn off the devices once you are done working on it

10. *Responsibilities of Staff and Parents*

The expectations of students for using school Internet and IT systems are clearly outline above. To support students in this, the school also expects teachers and parents to play a role.

School Staff

- All staff (teachers, leadership and administration) are expected to support acceptable use within the school and to model good practice.
- Staff are expected to support students at all times in their use of technology and to provide guidance and direction where needed. This will be in specified classes and training sessions along with any opportunities that arise in or out of class.
- Staff are required to report any unacceptable use to the school leadership and any other relevant authorities where necessary.

Parents

- All parents are expected to support acceptable use within the school and to model good practice.
- Parents are expected to support their children at all times in their use of technology and to provide guidance and direction where needed and where possible. If they are not able to guide their child in any aspect of acceptable use, they must contact the school for assistance.
- Parents are required to report any unacceptable use to the school immediately so that further action can be taken

11. Acceptable use for students (Guidelines)

- Communicate only in ways that are kind and respectful
- Communicate only with people you know and only through sanctioned platforms
- Communicate with teachers and other members only through official school platforms
- Avoid spam, chain letters, or other mass unsolicited mailings
- Always keep your home address or telephone numbers private
- Take action if you receive any message that is inappropriate or makes you feel uncomfortable. You should immediately inform an adult you trust which should be a parent, teacher, supervisor or social worker
- Speak out against cyber bullying (towards you and others) and immediately contact the relevant staff, parents, supervisor or social worker
- Respect yourself and all other users through good network etiquette
- Saying no to plagiarism and give credit to anyone whose work you are using for school purposes
- Helping to raising awareness across school of acceptable and smart use of internet
- Using the internet for educational purposes of research and information gathering from various websites and databases
- Using the school online platform for sharing documents and assignments for collaborative work
- Keeping your allocated personal username and password confidential, not sharing with anyone
- Accessing examination sites for practice papers and answer schemes
- Responsibly accessing social websites for educational purposes only under teachers'
- guidance
- Always using appropriate language in all digital communications through emails, social websites, blogs or messages
- Taking good care of all digital devices including the school network

12. Unacceptable use for students (Guidelines)

- Accessing, transmitting, copying, or creating material that violates the school's behavior policy (such as messages/content that are pornographic, sites that promote hatred, discrimination, racism, or meant to harass others)
- Accessing, transmitting, copying, or creating material that is illegal (such as inappropriate or obscene materials, stolen materials, or illegal copies of copyrighted works)
- Using internet to commit any kind of piracy such as music, film or software
- Using resources to further other acts that are criminal or violate the school's

- behavior policy
- Using emails, social media, texts or other online platforms to threaten or harass others
- Distributing any information which is incorrect, offensive or slanderous □ Using threatening and inappropriate language in communications
- Instigating or being involved in cyber bullying
- Not reporting cyber bulling when you are aware of it
- Planning or arranging appointments with anyone you have met on the internet
- Sending or posting disturbing images on any online platform
- Sharing passwords or using and distributing passwords of others
- Compromising the security of the school's systems by introducing malicious software
- Visiting unauthorized websites
- Damaging or interfering with computers, computer systems, software, or networks
- Deliberately causing harm to someone's work or program
- Changing another person's username, password, files or data
- Using someone else's information or work without permission (plagiarism)
- Disclosing personal information about yourself without authorization
- Visiting social websites without authorization
- Violating acceptable use agreements

13. Netiquette

- Users should not attempt to open files or follow links from unknown or untrusted origin.
- Recognizing the benefits collaboration brings to education
- Playing commercial/online games and visiting sites not related to education is not permitted.
- Respect the use of copyrighted materials. Respect the rights and privacy of others. □ Downloading of unauthorized programs is not allowed.
- Avoid modifying or copying any protected system files, system folders, or control panel files onschool equipment.
- Obey the laws and restrictions of UAE, do not use personal equipment to record (audio/visual) of others without their/ school permission and upload them on social media.
- Alert a teacher or other staff member if I see threatening, appropriate, or harmful content (images, messages, posts) online and help maintain the integrity of the school network.
- You should use trusted sources when conducting research via the Internet.

14. Personal Safety

- Students should not share personal information, including phone number, address, ID number,passwords or birthday over the internet without adult permission.
- Students should recognize that communicating over the internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others.
- Students should not agree to meet someone they met online in real life without parental permission.
- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher if you're at school; parent if you're using the device at home) immediately.
- Students should always use the internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognize that some valuable content online is unverified, incorrect, or inappropriate.
- Students should avoid any irrelevant post online that they would not want parents, teachers,future colleges, employers or the UAE government to see.

15. Acceptable/ Unacceptable Use of User Owned Devices

Cyber bullying/ social media

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyber bullying.

Students should not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber bullying can be a crime. Remember that your activities are monitored and retained.

Students will be held accountable for Cyber-Bullying, even if it occurs off-campus during the school year and negatively impacts the school environment. Students are reminded that in the UAE there are extreme consequences for online defamation of character of person or organization.

The UAE Student Conduct Disciplinary Bylaw and the Federal Decree-Law no. (5) outline that deliberately creating, transferring and publishing photos and comments on social media (Instagram and WhatsApp) that undoubtedly shows defamation of individuals or staff members, or School Leadership of character, dignity and integrity are breaking the law.

Key provisions relevant to schools' excerpts of Federal Decree-Law no. (5) state:

21	Invasion of privacy, including photographing others, or creating, transferring, disclosing, copying or saving electronic photos (just taking a photo or video of someone without their permission, or saving a photo they have posted, is enough). Defamation. Publishing news, photos, scenes, comments, statements or information, even if true and correct. Amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy.	Up to 6 months' imprisonment +/fine of AED 150k – 500k

All members of the SSAD community are expected to uphold the values of the school in all Social Media interactions.

Staff, students and parents will not act in such a way that the image of the school is brought into disrepute nor in a way that harms members of the school community. Therefore, it is expected that SSAD staff, students and parents use social media in a respectful and responsible manner. Social media should not be used to insult, present offensive or inappropriate content or to misrepresent SSAD or any member of the school community. Social media includes blogs, wikis, podcasts, digital images and video, instant messaging and mobile devices.

When using social media, students are expected to ensure that they:

- Read and agree to the terms and conditions of various social media sites as many of them have age restrictions for their use.
- Are aware of what they are posting online, and that Social Media sites and applications are public forums.
- Are not permitted to join a staff member's areas on networking sites unless pre- approved by administrator. If students attempt to do this, the member of staff refuses the student access and inform the Supervisor. The student's parents will be informed if this happens.
- Will not access social networking sites during the working days without permission from a teacher or supervisor
- Respect the rights and confidentiality of others.
- Do not impersonate or falsely represent another member of the school community.
- Do not bully, intimidate abuse, harass or threaten other members of the school community.
- Do not make defamatory comments toward other members of the school community.
- Do not use offensive or threatening language or resort to personal abuse toward each other or members of the school community.
- Do not harm the reputation of RISS or those within its community

- Do not upload video, audio or photographs of any member of the RISS community (student, parents or staff).
- To help ensure student safety and citizenship in online activities, all students will be educated about appropriate behavior, including interacting with other individuals on social networking websites, gaming, instant messaging, video messaging, chat rooms, and cyber-bullying awareness, plagiarism and response.

16. New employees and students

All users remain informed of our expectations and appropriate usage of resources through Induction program.

The E-safety team will:

- ensure all new students and staff receive access to age- appropriate IT resources and tools during the enrollment and hiring process, as well as on-going training in their safe, responsible, and effective use.
- Provide orientation for students and staff on IT resources and the school system.

In order to initiate and maintain access to IT resources, all students and staff must submit a signed Acceptable Use Agreement, non-adherence of which may result in loss of non-course related access and/or appropriate disciplinary and/or legal action. Violations are deemed as violations of school behavioral expectations and policies.

Students are expected to use all computer equipment, both hardware and software and network access to pursue intellectual activities, to seek resources, to access libraries and for other types of learning activities. They will learn new things and can share their newfound knowledge with classmates, teachers, parents and global learning partners. For the safety of all involved, caution must be exercised. Because SSAD network is used as part of a school activity, the policy on student behavior applies to network activity. Therefore, the Acceptable Use Policy is an extension of the school behavior Management Policy. These rules apply to vandalism of computer equipment, unauthorized access to information, computer piracy, hacking, tampering with hardware and software, bullying and harassment.

Student Behavior:

- Filtering should be used in conjunction with:

Educating students concerning the dangers of inappropriate material on the Internet.

- Using recognized Internet gateways as a searching tool and/or homepage for students, in order to:
    - Facilitate access to appropriate material
    - Using the school's "Acceptable Use" agreement
    - Using behavior management practices for which Internet access privileges can be earned or lost.
    - Appropriate supervision, both in person and/or electronically.

Prohibited use for all users

- Accessing other person's system, account or email
- Visiting unauthorized websites
- Passing any information that is offensive or incorrect
- Violating copyright law
- Sharing passwords or convincing others to share their password
- Deliberately causing harm to other person's work or data
- Intentionally breaching the school's security
- Using inappropriate language online
- Getting involved in cyber bullying
- Indulging in plagiarism

Roles and responsibilities for student Internet Safety

Students will:

- ensure they do not divulge any information about themselves or other persons on social media or through any other form of electronic communications over the Internet
- not disclose their home address or telephone numbers
- never upload any images of themselves or others without permission of parents or staff
- not plan or arrange appointments with anyone they have met on the Internet
- take proper measures if they receive any message that is inappropriate or makes them feel uncomfortable. They should immediately inform an adult they trust
- ensure they are not exposed to information or images that might harm them or cause them discomfort
- speak out against cyber bullying and immediately get in touch with the relevant Staff or parents
- avoid trying to access websites that have adult content and are restricted
- not damage computers, computer systems, software, or computer networks
- respect themselves and all other users through good network etiquette
- say no to plagiarism and give due credit to anyone whose work they are using for educational purposes
- help in raising awareness across School of acceptable and smart use of internet

Staff will:

- educate students about appropriate and safe Internet usage, including interaction and communication with other people on social networking websites and in chat rooms

- encourage awareness about cyber bullying and give clear guidelines as to the steps that are to be taken and people that can be approached
- monitor and ensure that there is no misuse of Internet
- raise awareness about the advantages and disadvantages of using social media like Facebook, Twitter, YouTube, Google+, and Instagram.
- use the online web-based interactive communication technologies to enhance students' education and learning and to facilitate collaborative study habits in students
- improve peer collaboration and sharing of Internet resources through sustained usage of online web-based interactive communication
- empower students with 21st century learning tools to enable them to become independent learners
- share outstanding teaching practices through electronic communication
- develop cross country collaboration in students encouraging knowledge and skill-based projects
- incorporate IT in all areas of the curriculum to encourage the holistic approach of the students
- develop presentation skills using IT for project work and competitions

Parents will:

- monitor and enforce their own family values to their children making them aware of the importance of using Internet safely
- involve their children in regular discussions regarding the different challenges that are presented through the Internet
- ensure that the children are aware of the acceptable Internet discipline and the consequences if the rules are broken
- maintain clarity and consistency on what is permissible and what activities are unacceptable
- assume complete responsibility for monitoring their children's use of Internet at home and outside School
- have complete awareness of cyber bullying and ensure that the children are not being subjected to it in any form through monitoring and discussions
- inform and work with the school if any misuse is reported or found
- seek help and support from the school in case of any incident that involves cyber bullying
- be well informed about the work or projects given to the children to rule out any misuse. In case of any concerns, they should check with the school immediately.

17. Promotion of the Policy

The policy will be promoted through circulars and workshops for parents and students throughout the school. The message will be reinforced periodically by all teachers. Parents will be reminded through posters and informative circulars. Competitions revolving around raising awareness on this and related

topics would definitely benefit. In Staff the policy would be promoted through workshops and focus group discussions. All users must sign Acceptable use agreements. It is clear to the staff that Acceptable use forms part of their employment contract.

18. Violations of this Policy

Violations of this policy may have disciplinary repercussions, including:

- The school reserves the right to terminate any user's access to School's Internet Systems - including access to School e-mail - at any time.
- If a student violates this policy, appropriate disciplinary action will be taken consistent with the Discipline policy of the School and UAE by law for Student Code of Conduct.
- If a student's access to the Department's Internet System is revoked, the student may not be penalized academically, and the Department will ensure that the student continues to have a meaningful opportunity to participate in the educational program.
- Staff violations of this policy will be handled by suitable disciplinary measures.
- All users must promptly disclose to their teacher, parent, or line manager about any information they receive that is improper or makes them feel uneasy.
- Removal of Internet and IT Systems privileges for a period of time
- Temporary/Permanent removal of the students from school
- Temporary/Permanent removal of staff from school
- Suspension/Termination from school after investigation process
- Referral to the relevant authorities

19. Reporting

All members of the school community are required to report any Unacceptable Use of technology within the school or on the school Internet or IT Systems. Any student or staff should report any Unacceptable Use or Cyber Bullying to the supervisor or to the social worker

20. Communication of this Policy

- Included in induction materials at the beginning of the year and for new Students and Staff
- Promoted and supported through the school's Online Safety Curriculum
- Promoted in all classes by all teachers
- Agreement signed by students, staff and parents and stored in file
- Attached to part of staff contract
- Included in trainings for all users

Onboarding – Acceptable Usage Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognize the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications technologies such as email, chat, social networking, gaming, instant messaging and video conferencing, this includes use of such systems outside of employment within school.
- I understand that risk associated with the above systems and will be a responsible user both inside school and outside of school.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, iPads etc) and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies set down by the school and systems have appropriate settings, filters and monitoring to protect learners from harmful online material without over-blocking.
- I will ensure I create a secure password for school technology and communication systems; one that could not easily be guessed by another person.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will be professional in my communications and actions when using school ICT systems.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and

in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Any images taken will be removed from my personal equipment before I go offsite. Where these images are published (e.g. on the school website / school app) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social media and networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I understand that failure to comply with this policy will immediately call into question my motivation for private communication with a child, and that this will be dealt with as a safeguarding issue in accordance with management procedures.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the ADEK and relevant UAE authorities have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will lock my laptop/desktop screen when not in use.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the UAE Cyber-Crime Law (Federal Law No. 34 of 2021) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others. Where digital personal data is transferred outside the secure local network, it must be encrypted. This includes the use of memory sticks and external hard drives. Paper-based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of systems and equipment off the premises and my use of school digital technology, including off-site and outside normal working hours.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Principal / Board and / or ADEK and relevant UAE authorities and in the event of illegal activities the involvement of the police.

I have read and understand the above, read the Responsible usage policy and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ----------

Position: ----------

Signed: ----------

Date: ----------

IT DEPARTMENT

Students Responsible Usage Policy

School landline : 02 31 01 888 School P.O Box: 63797
www.spanishschool.ae info@spanishschool.ae

1. Introduction

The Spanish School of Abu Dhabi makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the school by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the school, its students and its employees. This Acceptable Use policy is intended to minimize the likelihood of such harm by educating school users and setting standards which will serve to protect the school. The school firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

2. Aim

The aim of the Responsible use policy is to ensure that all Students and Parents are aware of the risks of internet usage and use it sensibly and safely for the purpose of information sharing and improved learning. All students should know about the Responsible use of technologies. All students should be free of any fear of cyber bullying by anyone known or unknown, should be able to recognize cyber bullying and be fully equipped to be able to deal with it effectively as well as are fully competent in surfing internet safely.

3. Principles of Acceptable and Safe Internet Use

- The school places ownership on all internet data that is produced, received or transmitted. This data can be revealed for appropriate requirement such as legal matters or investigative matters.
- All electronic paraphernalia both hardware and software, expertise and services involved in the usage of internet belong to the School and the School has the right to access and monitor all data and internet interchange.
- All emails sent through the school email system might be monitored to discourage use of offensive mails.
- All sites and downloads may be monitored or blocked by school if the school considers them.
- unsuitable or they are thought to be damaging to the school students.
- students should simply know “Don’t install anything without a teacher’s permission.
- Usage of storage media which is not scanned prior to usage is strictly prohibited in order to limit spread of Viruses and other malicious software.

4. Acceptable uses of the school’s internet systems

- Using the web browsers for educational purposes of research and information gathering from various websites and databases.
- Using the internet for sharing documents and assignments promoting collaborative work.
- Keeping the allocated personal username and password confidential, not sharing with anyone.

- Not trying to access and change any other person's username, password, files or data.
- Sharing emails only with people known to oneself and approved by parents or teachers.
- Using internet to do online tests or tasks approved or advised by the teachers.
- Studying syllabus content online and performing tasks pertaining to it with teachers' authorization.
- Doing projects or presentations for the lessons.
- Preparing circulars, invitations, information pamphlets for community service or other school activities with the teachers' approval.
- Accessing examination sites for practice papers and answer schemes.
- Responsibly accessing social websites for educational purposes only under teachers' guidance.
- Always using appropriate language in all digital communications through emails, socialwebsites, blogs or messages
- Taking good care of all digital devices in use

5. *Prohibited Uses of the School's Internet System*

- Using emails to threaten or harass other people
- Sending or posting disturbing images on the internet
- Using internet to commit any kind of piracy like music, film or software ▫ Sharing passwords or using and distributing passwords of others
- Violating the copyright law with respect to downloading or copying electronic files for personalusage
- Sharing School's confidential matters or information without authorization
- Compromising the security of the electronic system of the School by introducing malicious software
- Using the internet to promote personal business ▫ Visiting unauthorized websites
- Distributing any information which is incorrect, offensive or slanderous ▫ Using threatening and inappropriate language in communications
- Damaging the hardware or software
- Deliberately causing harm to someone's work or program
- Involving in cyber bullyingIndulging in plagiarism
- Accessing pornographic sites or sites that promote hatred, discrimination, racism ▫ Disclosing personal information about oneself without authorization
- Visiting social websites without authorization
- Using someone else's information, images of work without permission

6. Acceptable uses of the school's technology systems

- School devices are the sole property of the school, and all users will follow this policy
- School devices are intended for educational use only
- Any school device can be used only after the respective teacher has permitted use
- Music and internet games on school devices are allowed at the discretion of the teacher
- Games, apps, software, screen saver, backgrounds etc. should not be downloaded on school devices without permission from school.
- Do not change any device settings without permission from school
- Turn off all devices after you are done working on it
- All devices should be used in a responsible manner
- Do not write or label on school devices
- Any damage to the school devices will lead to disciplinary action by school administration.

7. Responsibilities of Parents

- All parents are expected to support acceptable use within the school and to model good practice.
- Parents are expected to support their children at all times in their use of technology and to provide guidance and direction where needed and where possible. If they are not able to guide their child in any aspect of acceptable use, they must contact the school for assistance.
- Parents are required to report any unacceptable use to the school immediately so that further action can be taken

8. Acceptable use Guidelines

- Communicate only in ways that are kind and respectful
- Communicate only with people you know and only through sanctioned platforms
- Communicate with teachers and other members only through official school platforms
- Avoid spam, chain letters, or other mass unsolicited mailings
- Always keep your home address or telephone numbers private
- Take action if you receive any message that is inappropriate or makes you feel uncomfortable. You should immediately inform an adult you trust which should be a parent, teacher, supervisor or social worker
- Speak out against cyber bullying (towards you and others) and immediately contact the relevant staff, parents, supervisor or social worker

- Respect yourself and all other users through good network etiquette
- Saying no to plagiarism and give credit to anyone whose work you are using for school purposes
- Helping to raising awareness across school of acceptable and smart use of internet
- Using the internet for educational purposes of research and information gathering from various websites and databases
- Using the school online platform for sharing documents and assignments for collaborative work
- Keeping your allocated personal username and password confidential, not sharing with anyone
- Accessing examination sites for practice papers and answer schemes
- Responsibly accessing social websites for educational purposes only under teachers'
- guidance
- Always using appropriate language in all digital communications through emails, social websites, blogs or messages
- Taking good care of all digital devices including the school network

9. *Unacceptable use Guidelines*

- Accessing, transmitting, copying, or creating material that violates the school's behavior policy (such as messages/content that are pornographic, sites that promote hatred, discrimination, racism, or meant to harass others)
- Accessing, transmitting, copying, or creating material that is illegal (such as inappropriate or obscene materials, stolen materials, or illegal copies of copyrighted works)
- Using internet to commit any kind of piracy such as music, film or software
- Using resources to further other acts that are criminal or violate the school's
- behavior policy
- Using emails, social media, texts or other online platforms to threaten or harass others
- Distributing any information which is incorrect, offensive or slanderous □ Using threatening and inappropriate language in communications
- Instigating or being involved in cyber bullying
- Not reporting cyber bulling when you are aware of it
- Planning or arranging appointments with anyone you have met on the internet
- Sending or posting disturbing images on any online platform
- Sharing passwords or using and distributing passwords of others
- Compromising the security of the school's systems by introducing malicious software

- Visiting unauthorized websites
- Damaging or interfering with computers, computer systems, software, or networks
- Deliberately causing harm to someone's work or program
- Changing another person's username, password, files or data
- Using someone else's information or work without permission (plagiarism)
- Disclosing personal information about yourself without authorization
- Visiting social websites without authorization
- Violating acceptable use agreements

10. Personal Safety

- Students should not share personal information, including phone number, address, ID number,passwords or birthday over the internet without adult permission.
- Students should recognize that communicating over the internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others.
- Students should not agree to meet someone they met online in real life without parental permission.
- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher if you're at school; parent if you're using the device at home) immediately.
- Students should always use the internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognize that some valuable content online is unverified, incorrect, or inappropriate.
- Students should avoid any irrelevant post online that they would not want parents, teachers,future colleges, employers or the UAE government to see.

11. Acceptable/ Unacceptable Use of User Owned Devices

Cyber bullying/ social media

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyber bullying.

Students should not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber bullying can be a crime. Remember that your activities are monitored and retained.

Students will be held accountable for Cyber-Bullying, even if it occurs off-campus during the school year and negatively impacts the school environment. Students are reminded that in the UAE there are extreme consequences for online defamation of character of person or organization.

The UAE law outline that deliberately creating, transferring and publishing photos and comments on social media (Instagram and WhatsApp) that undoubtedly shows defamation of individuals or staff members, or School Leadership of character, dignity and integrity are breaking the law.

All members of the SSAD community are expected to uphold the values of the school in all Social Media interactions.

Students and parents will not act in such a way that the image of the school is brought into disrepute nor in a way that harms members of the school community. Therefore, it is expected that SSAD students and parents use social media in a respectful and responsible manner. Social media should not be used to insult, present offensive or inappropriate content or to misrepresent SSAD or any member of the school community. Social media includes blogs, wikis, podcasts, digital images and video, instant messaging and mobile devices.

When using social media, students are expected to ensure that they:

- Read and agree to the terms and conditions of various social media sites as many of them have age restrictions for their use.
- Are aware of what they are posting online, and that Social Media sites and applications are public forums.
- Are not permitted to join a staff member's areas on networking sites unless pre- approved by administrator. If students attempt to do this, the member of staff refuses the student access and inform the Supervisor. The student's parents will be informed if this happens.
- Will not access social networking sites during the working days without permission from a teacher or supervisor
- Respect the rights and confidentiality of others.
- Do not impersonate or falsely represent another member of the school community.
- Do not bully, intimidate abuse, harass or threaten other members of the school community.
- Do not make defamatory comments toward other members of the school community.
- Do not use offensive or threatening language or resort to personal abuse toward each other or members of the school community.
- Do not harm the reputation of RISS or those within its community
- Do not upload video, audio or photographs of any member of the RISS community (student, parents or staff).
- To help ensure student safety and citizenship in online activities, all students will be educated about appropriate behavior, including interacting with other individuals on social networking websites, gaming, instant messaging, video messaging, chat rooms, and cyber-bullying awareness, plagiarism and response.

12. New students

All users remain informed of our expectations and appropriate usage of resources through Induction program.

The school will:

- ensure all new students receive access to age- appropriate IT resources and tools during the enrollment and hiring process, as well as on-going training in their safe, responsible, and effective use.
- Provide orientation for students on IT resources and the school system.

In order to initiate and maintain access to IT resources, all students' parents must submit a signed Acceptable Use Agreement, non-adherence of which may result in loss of non-course related access and/or appropriate disciplinary and/or legal action. Violations are deemed as violations of school behavioral expectations and policies.

Students are expected to use all computer equipment, both hardware and software and network access to pursue intellectual activities, to seek resources, to access libraries and for other types of learning activities. They will learn new things and can share their newfound knowledge with classmates, teachers, parents and global learning partners. For the safety of all involved, caution must be exercised. Because SSAD network is used as part of a school activity, the policy on student behavior applies to network activity. Therefore, the Acceptable Use Policy is an extension of the school behavior Management Policy. These rules apply to vandalism of computer equipment, unauthorized access to information, computer piracy, hacking, tampering with hardware and software, bullying and harassment.

Student Behavior:

- Filtering should be used in conjunction with:

Educating students concerning the dangers of inappropriate material on the Internet.

- Using recognized Internet gateways as a searching tool and/or homepage for students, in order to:
    - Facilitate access to appropriate material
    - Using the school's "Acceptable Use" agreement
    - Using behavior management practices for which Internet access privileges can be earned or lost.
    - Appropriate supervision, both in person and/or electronically.

Prohibited use for all users

- Accessing other person's system, account or email
- Visiting unauthorized websites
- Passing any information that is offensive or incorrect
- Violating copyright law

- Sharing passwords or convincing others to share their password
- Deliberately causing harm to other person's work or data
- Intentionally breaching the school's security
- Using inappropriate language online
- Getting involved in cyber bullying
- Indulging in plagiarism

Roles and responsibilities for student Internet Safety

Students will:

- ensure they do not divulge any information about themselves or other persons on social media or through any other form of electronic communications over the Internet
- not disclose their home address or telephone numbers
- never upload any images of themselves or others without permission of parents or staff
- not plan or arrange appointments with anyone they have met on the Internet
- take proper measures if they receive any message that is inappropriate or makes them feel uncomfortable. They should immediately inform an adult they trust
- ensure they are not exposed to information or images that might harm them or cause them discomfort
- speak out against cyber bullying and immediately get in touch with the relevant Staff or parents
- avoid trying to access websites that have adult content and are restricted
- not damage computers, computer systems, software, or computer networks
- respect themselves and all other users through good network etiquette
- say no to plagiarism and give due credit to anyone whose work they are using for educational purposes
- help in raising awareness across School of acceptable and smart use of internet

Parents will:

- monitor and enforce their own family values to their children making them aware of the importance of using Internet safely
- involve their children in regular discussions regarding the different challenges that are presented through the Internet
- ensure that the children are aware of the acceptable Internet discipline and the consequences if the rules are broken
- maintain clarity and consistency on what is permissible and what activities are unacceptable
- assume complete responsibility for monitoring their children's use of Internet at home and outside School

- have complete awareness of cyber bullying and ensure that the children are not being subjected to it in any form through monitoring and discussions
- inform and work with the school if any misuse is reported or found
- seek help and support from the school in case of any incident that involves cyber bullying
- be well informed about the work or projects given to the children to rule out any misuse. In case of any concerns, they should check with the school immediately.

13. Violations of this Policy

Violations of this policy may have disciplinary repercussions, including:

- The school reserves the right to terminate any user's access to School's Internet Systems - including access to School e-mail - at any time.
- If a student violates this policy, appropriate disciplinary action will be taken consistent with the Discipline policy of the School and UAE by law for Student Code of Conduct.
- If a student's access to the Department's Internet System is revoked, the student may not be penalized academically, and the Department will ensure that the student continues to have a meaningful opportunity to participate in the educational program.
- Staff violations of this policy will be handled by suitable disciplinary measures.
- Removal of Internet and IT Systems privileges for a period of time
- Temporary/Permanent removal of the students from school
- Referral to the relevant authorities

14. Reporting

All students are required to report any Unacceptable Use of technology within the school or on the school Internet or IT Systems. Any student should report any Unacceptable Use or Cyber Bullying to the supervisor or to the social worker

Middle School – Acceptable Usage Agreement

I understand that the Spanish school of Abu Dhabi provides electronic resources, including Internet access and storage space for students' work, as an integral part of the curriculum. Behavior and language in the use of these resources should be consistent with classroom standards. I agree to the following responsibilities and restrictions:

1. I will use the electronic resources, including storage space, only for educational purposes related to work in RISS, and not for any personal, commercial or illegal purposes.
2. I will use the Internet only with the permission of the teacher or staff member in charge.
3. I will not use games or other electronic resources that have objectionable content or that engage me in an inappropriate simulated activity.
4. I will not give my password to any other user, nor attempt to learn or to use anyone else's password, and I will not transmit my address or telephone number, or any personal or confidential information about myself or others.
5. I will not upload, link, or embed an image of myself or others to non-secured, public sites without my teacher's permission and a signed parental permission slip.
6. I will not make statements or use the likeness of another person through website postings, email, instant messages, etc., that harass, intimidate, threaten, insult, libel or ridicule students, teachers, administrators or other staff members of the school community, make statements that are falsely attributed to others, or use language that is obscene.
7. I will not violate copyright laws, damage or tamper with hardware or software, vandalize or destroy data, intrude upon, alter or destroy the files of another user, introduce or use computer "viruses," attempt to gain access to restricted information or networks, or block, intercept or interfere with any email or electronic communications by teachers and administrators to parents, or others.
8. I will not use, or create for others, any program to interfere with, change, or interact with programs, security settings, systems, or devices that are the property of the RISS and are used for school-related purposes by students, their parents and staff.
9. I will not imply, directly or indirectly, either publicly or privately that any program or "app" I create is associated with, or a product of RISS nor will I either directly or indirectly associate any such program with anyRISS logos or images.
10. I understand that my use of the school system's computers is not private, and that the school reserves the right to monitor use to assure compliance with these guidelines; violations may lead to revocation of computer access and/or other disciplinary measures**.**
11. I understand that the prohibited conduct described above is also prohibited off campus when using private equipment if it has the effect of seriously interfering with the educational process, and that

such off-campus violations may lead to disciplinary measures.

12. Plagiarism is serious. I will not post work or thoughts of others without permission and crediting their work.
13. I will report any problems to the supervising staff member.

Violation of this policy

The school will use available monitoring and blocking software to filter inappropriate material on the Internet. Student violations of this policy may result in loss of access as well as other disciplinary or legal actions, which may include:

- Financial payment to repair/replace lost/damaged equipment/systems/data/services.
- Loss of privileges - email, network, system account, IPad/laptop/computer/mobile use, etc.
- Suspension from school (for severe violations)
- Expulsion from school and/or legal action and action by the authorities (for severe violations)

☑ In any specific incident, the school administration makes the final decision as to what is and is not a violation of the policy and also decides when school expulsion and/or legal actions by the authorities are the appropriate course of action.

☑ I understand that it is my responsibility to follow the policy online, offline, at school and at home. I have read & understood the policy and agree to follow the above guidelines.

Student's Name:_____

Grade: _____**Student's Signature:**_____ **Date:**_____

Parents: I have read, understood, and discussed with my son or daughter this Responsible Use Policy, and I give him or her permission to use electronic resources, understanding that this access and use of personal devices on school grounds is conditional upon adherence to the agreement.

Although students are supervised when using school resources, and their use of school resources is electronically monitored, I am aware of the possibility that my son or daughter may gain access to material that school officials, and I may consider inappropriate or not of educational value.

Parent's Name: _____

Parent's Signature:_____**Date:**_____

Digital Media Policy And Social Media Policy

School landline : 02 31 01 888 School P.O Box: 63797
www.spanishschool.ae info@spanishschool.ae

Digital Media Policy and Social Media Policy

8.1 Digital Media Policy

The Spanish School of Abu Dhabi has developed, implemented, and oversees a Digital Media Policy that regulates the creation and publication of digital content. This policy includes:

1. **Obtaining prior consent for recording and publishing digital media:**
   a. The school may only take photographs and/or video recordings of students after obtaining written consent from parents or guardians. When obtaining such consent, the school will inform them of the purposes of the photographs and/or recordings.
   b. Before publishing digital content that includes students, the school must have written parental consent, specifying whether the student will be identified by name.

2. **Procedures for providing and withdrawing consent:**

   - Consents will be collected at the time of enrollment through an official document and will be stored by the Admissions Officer.
   - Parents may withdraw their consent at any time by submitting a written request to the school administration.

3. **Conditions for storing and securing digital media:**

   - All digital material involving students must be stored on secure servers and comply with UAE data-protection legislation and ADEK guidance.
   - Access is restricted to authorized personnel in line with the L1–L5 authorisation matrix.
   - Access to these files will be restricted to authorized personnel.

4. **Use of personal devices and accounts for recording or publishing school content:**

   - Employees shall not record or publish school-related content on their personal devices or accounts without the express authorization of the school administration. **Employees must use the devices provided by the school to record or take any photographs of students.**

5. **Protocol for the deletion of published digital content:**

   - If a deletion request is submitted, the school will review the request and proceed with the deletion within a maximum period of seven calendar days.
   - The requester will be notified once the content has been removed.

8.2 Social Media Policy

Schools must develop and implement a Social Media Policy that regulates its use within the educational environment. This policy must include, at a minimum:

1. **Official platforms and accounts:**
    - The school may use various platforms without restrictions, depending on its needs.
    - All official accounts will be managed by the Social Media Coordinator, with occasional technical support.
2. **Security and access:**
    - Official account passwords will be securely managed and shared only with authorized personnel.
    - Passwords for official accounts are handled under the same complexity and MFA requirements defined in the cybersecurity policy.
3. **Content and language guidelines:**
    - All published content must be professional, respectful, and aligned with ADEK's values and ethics.
4. **Use of students' names, photos, and videos:**
    - The consent criteria described in Section 8.1 will apply.
5. **Content moderation:**
    - The school will designate moderators to review and, if necessary, remove third-party content that is inappropriate or contrary to ADEK's values.
6. **Procedures for managing incidents on social media:**
    - Impersonation, harassment or other adverse behaviours are escalated to the IT Department and the Well-being Coordinator for investigation within the framework of the *Incident Response Plan*.

8.3 Staff Personal Accounts

Teaching and administrative staff may have personal social media accounts, but they must adhere to the following guidelines:

1. Do not use school email addresses to create personal accounts.
2. Set privacy settings to the most restrictive options.
3. Do not identify as school employees, except on professional platforms such as LinkedIn.
4. Do not accept or send connection requests to students or former students under the age of 18.
5. Do not accept connection requests from parents of current students.
6. Do not use personal social media to communicate with students or families.
7. Ensure that all published content is appropriate and aligned with ADEK's values.
8. Do not disclose confidential information about the school.

8.4 Email Communications

1. A formal and professional tone is required in all email communications.
2. Only authorized personnel may send emails to the entire educational community.
3. Backup and Archiving
   • All e-mail is automatically backed up to encrypted cloud storage (Google / Microsoft).
   • Messages are retained for **seven years** in compliance with ADEK and UAE record-keeping rules before secure deletion. (Concrete retention period added in line with the backup standards.)

8.5 School Website

1. The school will maintain an up-to-date website that serves as a reference for the educational community.
2. The minimum required content will include:
   - Contact information.
   - Services provided by the school.
   - Fees, including transportation and optional activities.
   - Inspection reports.
   - Aggregate academic performance data or individual achievements (with consent).
   - School Directory.
   - Relevant school policies.
3. The information will be reviewed and updated at least once a year or whenever changes occur.