Al Sadiq Islamic English School

Digital Technology Policy

Policy Name	Digital Technology Policy 2025-26
Stakeholder	All staff, students, and parents
Policy Directory Reference	Al Sadiq Islamic English School
Policy Lead	Vice Principal - Ms.Aisha Thasneem, Ms.Georgina Drake
Reviewed by	Mr. Julian Williams
Approved by	Ms. Sadia Wajid – Principal
Approved Date	September 2025
Monitoring Cycle	Annually

Contents:

1. Bring Your Own Device (BYOD) Policy

Purpose

The Bring Your Own Device (BYOD) Policy has been designed to ensure that all members of the community are given the opportunity to develop the necessary skills and literacy to thrive in the digital age.

Student-centred learning is a key value of any British School and BYOD helps support this philosophy by giving students more opportunities to take responsibility for their own learning.

Scope

This policy applies to all teachers, assistants, students and parents in all departments and phases of the school.

Policy Statement

Al Sadiq Islamic English School is dedicated to providing a learning environment that gives access to appropriate technology in order to enhance learning, unlock potential and connect students locally and globally. We ensure that all students, teachers, administration staff and guests have access to high-speed internet in all areas of the school.

Procedures & Implementation

The students at ASIES are digital-natives. For them, technology is part of the environment in which they are growing up, not just a resource.
Our aim at ASIES is for students to learn with technology, rather than learning from technology.
The use of BYOD supports key contemporary learning skills including:

- Accessing, filtering and processing information
- Planning and organising
- Making choices and decisions
- Facing challenges and problem solving
- Risk-taking and overcoming challenges
- Collaborating and sharing
- Communicating
- Being creative and innovative
- Reflecting

This policy applies to any device that is not school owned or supplied, and is used to access the school wireless network. The purpose of this policy is to establish clear guidelines and procedures when students use their own devices in school, to ensure safe use and the integrity of the ASIES network.

Which devices are suitable for BYOD?

This BYOD policy applies to all devices which fit the following classifications:

- Tablets
- Chromebooks
- Laptop/notebook computers

Smartphones are prohibited as per the school policy.

Usage

It is expected that all users of the network, digital resources will:

- Obey the laws and restrictions of the United Arab Emirates
- Respect other users in the School community, which includes the strict prohibition of cyberbullying and harassment
- Always use your own login account and password and not through any other individual's

- Do not disrupt, delete and tamper with someone else's work that is saved on school devices and network
- Recognise and honour the intellectual property of others
- Comply with legal restrictions regarding plagiarism, the use and citation of information resources and copyright law
- Limit the use of the school's technology resources to the educational vision and mission of the school
- Use non-curriculum relevant materials only in their own time, outside of school and without detriment to their studies
- Help maintain the integrity of the school network and equipment;
- Not tamper or experiment with the school network or equipment, including efforts to bypass the school's Internet filters or proxies
- Make personal devices available for inspection by an administrator or other staff member upon request;
- Use appropriate language in all communications
- Never use or attempt to use another student's assigned hardware, subscriptions, logins, files, or personal information
- Not give out personal information, such as name, address, photo, or other identifying information online, including username and password as this is prohibited
- Not use personal devices or equipment to record (audio/visual) others without their permission, as this is prohibited
- Not modify or copy any protected system files, system folders, or control panel files without prior approval of the School's IT Department
- Not install any software's that will compromise on the safety and security of the system such as VPNs, as this is prohibited
- Use the internet for educational and administrative purposes only. Use of the internet for emails and social networking sites is for only educational needs
- Inform the IT team before installing any software's on the school devices
- Use only licensed software for educational purposes
- Handle devices with care and be responsible for any loss or damage to individual devices
- Report any problems with the School equipment to the IT department

Users are not expected to:

- Store commercial software, music, games or any hidden files and folders on their devices
- Communicate between student and parents during the school time - in case of emergency parents should contact the school
- Store parents' files and folders on their devices
- Play games in school
- Download unlicensed software
- Repair, reconfigure, modify or attach any external devices to existing hardware without the permission of the IT department
- Infringe or violate UAE or international copyright laws or restrictions

Software / Apps:

Devices should have –

- A web-browser - All online devices already include a web browser like Safari, Internet Explorer, Firefox or Google Chrome.
- MS Office – including Microsoft Word, Excel and Powerpoint
- No games should be downloaded or accessible on the device
- No social media accounts
- No calling or messaging service should be accessible during school hours

Consequences

Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:

- Temporary confiscation of device
- Search of device contents to locate evidence of misuse
- Limitations, suspension, and/or revocation of access privileges to personal and school technology resources
- Disciplinary measures, up to suspension or expulsion
- Legal action and prosecution by relevant authorities, where applicable under UAE law

Roles and Responsibilities

All Users are responsible for:

- Submitting a signed Use of Electronic Devices Agreement prior to connecting to the school network
- Ensuring electronic devices are used in accordance with school policies and procedures
- Caring, maintaining, securing, and storing electronic devices; The School will take no responsibility for any loss or damage incurred whilst the Device is under the care of its user
- Preserving privacy of accounts, login names, passwords, and/or lock codes to maintain security of electronic devices and data
- Maintaining safe and productive learning environments when using electronic devices;
- Practicing digital citizenship

Principal and Senior Leaders:

- Create clear BYOD guidelines with input from teachers, parents, and students.
- Ensure the school's network can handle multiple devices.
- Provide technical support for device-related issues.
- Implement cybersecurity measures for the school network.
- Provide teachers with resources for integrating devices into their lessons.

Teachers:

- Creating equitable learning opportunities that include electronic devices for education purposes when relevant to curriculum and instruction
- Determining when students are able to use school or personal electronic devices for education purposes
- Supervising student use of electronic devices
- Responding effectively to disciplinary issues from inappropriate electronic device usage
- Communicating appropriately with administrators, parents, and students if school policy is violated from electronic device usage
- Teachers must continually supervise the content of what students are browsing inside the classroom
- Ensuring that Device use is supplementary to and supportive of other forms of learning, and that there are equitable opportunities to use devices alongside hand-writing in copybooks and workbooks

Students:

- Using electronic devices for educational purposes in approved locations under the supervision of school personnel only
- Implementing virus and malware scanning on their electronic devices
- Reporting any inappropriate electronic device usage to a teacher or administrator immediately
- Ensuring their electronic device is charged prior to bringing them to school
- Continuing to learn using an alternative method if an electronic device malfunctions
- Keep their device safe

Parents:

- Helping their children take all reasonable steps to care, maintain, secure, store, and transport their electronic device
- Helping their children preserve the privacy of accounts, login names, passwords, and/or lock codes
- Identifying the electronic device by labelling it, recording details such as make, model, and serial number, and/or installing tracking software
- Procuring hazard or theft insurance for an electronic device
- Encouraging their children to follow school policy and practice digital citizenship
- Contacting the school office to communicate with their child during the school day, instead of using text messages, emails, phone calls, or other digital means that have no curriculum-related/education purpose
- Assuming all responsibility for their child's unauthorised use of non-school Internet connections such as a 3G/4G cellular phone network

2. ICT Acceptable Use Policy

Purpose

This Acceptable Use Policy is intended:

- To promote the appropriate use of ICT by all members of the school community that ensures the safety and well-being of all students, staff and parents, emphasising a zero tolerance to cyberbullying
- To ensure students, staff and parents are aware of their roles and shared responsibilities in relation to cyber safety and appropriate online behaviours
- To develop the skills, knowledge, attitudes and behaviours required of students, staff and parents to participate and function responsibly, safely and appropriately in cyberspace
- To ensure all students and staff understand the importance of password security and the need to log out of accounts
- To create awareness among the stakeholders on 'the various initiatives of the UAE in relation to child protection by incorporating Wadeema's Law (Federal Law No. 3 of 2016) which sets out the precedent concerning child rights, and states that all children must be provided with appropriate living standards, access to health services, education, equal opportunities in essential services facilities without any kind of discrimination
- Combat Cyber Crimes (Federal Law No: 5 of 2012): The article of this law highlights a number of computer and online related activities and how they would be dealt with under the law. It addresses subjects such as IT security, invasion of privacy, malicious and illegal activities including hacking, fraud, improper system use, defamation, threats to state security, terrorism, insult to religions, and many more. etc. It will deal with incidents written within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/caregivers of incidents of inappropriate e-safety behaviour that take place outside of the school

Scope

This policy applies to:

- All students, staff, and parents/guardians using school ICT systems, networks, or devices.
- Personal devices (laptops, tablets) connected to the school's network under BYOD guidelines.
- Online behaviour, including social media activity, that impacts the reputation, safety, or well-being of students, staff, or the school community.

Subject Policy Statement

Al Sadiq Islamic English School embraces the presence and use of Information and Communication Technologies (ICT) as an integral part of the learning environment. The Cyber Safety policy seeks to ensure the safe and responsible use of ICT within Al Sadiq Islamic English School.

Procedures & Implementation

All users must:

- Use ICT resources for educational and professional purposes only.
- Respect the rights, dignity, and privacy of others online.
- Avoid any use of ICT that damages the school's reputation or disrupts its safe environment.
- Report immediately any inappropriate, harmful, or suspicious online activity.

User Identification and Passwords

- To log on, children and students are given a unique user identification (user-ID) that is protected by a secure password
- Passwords must be kept confidential
- Passwords must not be included in log-in scripts or other automated log-on processes
- Passwords must not be disclosed to unauthorised people
- Students will be accountable for any inappropriate actions (e.g. bullying, accessing or sending inappropriate material) undertaken by an unauthorised person using their password

Roles and Responsibilities:

Teachers:

Teachers at Al Sadiq Islamic English School are expected to use digital technology in a professional, safe, and responsible manner to protect both themselves and the students in their care.

Professional Use of Technology

- Use school digital systems, networks, and devices solely for educational purposes.
- Remain professional in all communications and online actions, both in and out of school.
- Use only personal logins and passwords, keeping them secure, and never attempt to access another user's account.
- Report immediately any illegal, inappropriate, or harmful content, incidents, or misuse.
- Never attempt to bypass security filters, disable equipment, or install unauthorised software.
- Ensure that all devices (school-owned or personal) used on the school network are virus-free, have up-to-date security software, and comply with school ICT rules.

Teaching and Monitoring

- Actively embed online safety into teaching and model safe use of digital technology.
- Provide students with opportunities to enhance learning through responsible use of ICT.

- Monitor students' use of school ICT systems, reporting concerns to the relevant safeguarding or IT lead.
- Ensure that students understand digital citizenship, including respect, privacy, and cyber safety.

Data Protection and Confidentiality

- Follow school and UAE data protection requirements when handling personal data.
- Transport, share, or disclose data only with appropriate authorisation and ensure it is password-protected or securely stored.
- Keep all staff and student information private and confidential unless disclosure is required by law or school policy.
- Back up data regularly and avoid storing confidential information on unsecured personal devices.

Digital Images and Media

- Only publish or share images or videos of students and staff in line with the school's Digital and Video Images Policy.
- Never use personal devices to record or photograph students.
- Respect copyright law by using and attributing original work appropriately, without downloading or distributing unlicensed material.

Social Media and Communication

- Use social media strictly in accordance with the school's Social Media Policy.
- Communicate with students and parents only via official school platforms, always maintaining a professional tone.
- Avoid any online activity, post, or interaction that could compromise professional responsibilities or the school's reputation.

Accountability and Compliance

- Understand that this policy applies both in school and when using school systems off-site, or personal devices on school premises.
- Accept responsibility for all actions when using digital technology linked to the school.
- Recognise that breaches of this policy may result in disciplinary action, including formal warnings, suspension, referral to school leadership or authorities, and, in cases of illegal behaviour, police involvement.

Students

Students at Al Sadiq Islamic English School are expected to use digital technology respectfully, safely, and only for educational purposes.

Responsible Use of Technology

- Use digital devices and school systems only for learning and in supervised, approved settings.
- Log in with personal credentials only and never attempt to access another user's account.
- Keep passwords and personal information private, and never share them with others.
- Report immediately to a teacher any inappropriate, unsafe, or harmful content, messages, or incidents.
- Use respectful language in all digital communications.

Safe and Legal Use

- Never attempt to bypass school security filters or tamper with devices or the network.
- Do not download or install unauthorised apps, software, or games.
- Avoid plagiarism by respecting copyright and properly crediting others' work.
- Understand that recording or photographing others without consent is strictly prohibited.
- Never engage in cyberbullying, online harassment, or any activity that causes harm to others.

Digital Citizenship

- Handle all devices carefully and take responsibility for their safe use.
- Use the internet for research, projects, and educational communication only.
- Avoid accessing social media, chat apps, or gaming platforms during school hours.
- Recognise that online actions have real-world consequences and reflect on the school community.

Accountability

- Students are responsible for their actions both in and out of school when using school-related digital platforms.
- Breaches of this policy may result in disciplinary action, including loss of ICT privileges, detention, suspension, or referral to external authorities in severe cases.

Parents

Parents and guardians play an essential role in supporting safe and responsible use of technology by their children.

Supporting Safe Use

- Ensure their child brings only approved devices (as per the BYOD Policy) and that these devices are secure, labelled, and in good working condition.
- Help their child keep passwords private and accounts secure.

- Monitor their child's use of devices at home, particularly internet use, social media, and communication platforms.
- Encourage balanced screen time and healthy digital habits to avoid electronic addiction.

Partnership with the School

- Communicate with their child during school hours only through official school channels, not through calls, messaging, or social media.
- Inform the school of any online safety concerns affecting their child.
- Support the school's policies on cyber safety, digital citizenship, and the prohibition of smartphones, gaming, and social media use in school.
- Ensure devices used for schoolwork have no unauthorised applications such as VPNs, chat apps, or games.

Accountability

- Accept responsibility for their child's unauthorised or inappropriate use of personal or external networks (e.g., mobile data).
- Understand that repeated misuse of digital technology may result in their child's access being limited or disciplinary action being taken.
- Work in cooperation with teachers and the school to model positive and respectful digital behaviour.

Complaints Procedures

Students, staff or parents can report any breaches of Use of Electronic Devices Agreement or incidents of cyberbullying activity to the Designated Safeguarding Team members at any time.

Any alleged incidences or allegations of behaviour that are in breach of the school's Use of Electronic Devices Agreement will be thoroughly investigated by the school.

- Significant breaches made by, or involving, students will result in the school notifying the parents of those students
- The school's response to alleged breaches will be followed up with due diligence and consideration for all parties involved or affected by any breach

The progress and well-being of any student involved in breaches will be monitored and evaluated in line with our Child Protection and Safeguarding Policy.
Where cyberbullying has been identified, counselling and support may be offered, as determined by the school.
Consequences of inappropriate use will follow the steps outlined in the Student Behaviour Policy.

3. Cyber Safety Policy

Purpose

The purpose of this Cyber Safety Policy is to ensure that all students, staff, and parents use digital technologies in a responsible, respectful, and safe manner. It seeks to protect members of our school community from cyber risks such as bullying, harassment, defamation, identity theft, and inappropriate use of technology, while promoting positive digital citizenship in line with UAE laws and cultural values.

Scope

This policy applies to all members of the school community – students, teachers, administrative staff, and parents – whenever they use:

- School-owned devices, networks, or internet connections.
- Personal devices (BYOD) connected to the school network.
- Any digital platform or social media that involves the school, its staff, or its students.

Policy Statement

Al Sadiq Islamic English School is committed to providing a safe digital learning environment. Cyber safety is the shared responsibility of the school, parents, and students. Any form of online misconduct, whether during school hours or outside, that impacts the reputation, wellbeing, or safety of the school community, will be addressed in line with school policies and UAE cyber laws.

Key Guidelines

Safe and Responsible Use of Technology

- Technology must only be used for educational purposes and with teacher supervision.
- Students must never share personal details (e.g., phone numbers, addresses, passwords, or photographs) online without parental consent.
- Students must not access inappropriate websites, apps, or online games through school devices or networks.
- The use of VPNs, proxy servers, or any method to bypass school filters is strictly prohibited.

Cyberbullying and Online Harassment

- Any use of digital platforms (e.g., social media, messaging apps, email, online forums) to threaten, harass, insult, or intimidate others is strictly forbidden.
- Cyberbullying includes:
    - Sending abusive or offensive messages.
    - Sharing embarrassing photos/videos without consent.
    - Excluding individuals from online groups to cause harm.
    - Spreading rumours or false information.
- All incidents of cyberbullying will be investigated, and consequences may include detention, suspension, removal of ICT privileges, and referral to external authorities if necessary.

Cyber Safety in Teaching and Learning

- Teachers must actively monitor students' online behaviour in class.
- Students may only use approved platforms such as Google Classroom, Microsoft Teams, Purple Mash, or other school-authorised applications.
- Recording or photographing teachers, students, or school activities without explicit permission is strictly prohibited.
- Students must report any inappropriate online content or behaviour immediately to a teacher or administrator.

Consequences of Breaches

Any violation of this Cyber Safety Policy may result in:

- Verbal or written warnings.
- Temporary or permanent removal of ICT privileges.
- Detentions, suspensions, or exclusions from school.
- Confiscation of devices.
- Referral to legal authorities under UAE law in severe cases (e.g., defamation, hacking, sharing explicit content).

Roles and Responsibilities

- School Leadership: Ensure cyber safety policies are implemented and reviewed annually.
- Teachers: Monitor and guide responsible ICT use in lessons, model positive digital citizenship.
- Parents: Supervise children's technology use at home, reinforce cyber safety, and raise concerns with the school promptly.
- Students: Use technology responsibly, report unsafe behaviour, and respect the rights of others online.

Training and Awareness

- Students: Regular workshops on cyberbullying, online safety, and respectful use of social media.
- Parents: Awareness sessions on monitoring devices, safe apps, and supporting digital wellbeing.
- Staff: Annual training on safeguarding, cyber safety protocols, and handling online incidents.

4. Defamation and Social Media Policy

Purpose

To safeguard the reputation, dignity, and wellbeing of all members of the Al Sadiq Islamic English School community by setting clear expectations regarding the responsible use of social media and other digital platforms.

Scope

This section applies to all students, parents, staff, and community members whenever they use social media or digital communication platforms, whether inside or outside school hours, if their actions:

- Refer to the school, its leadership, or staff members.
- Involve students of the school.
- Could directly or indirectly affect the reputation of the school or any of its community members.

UAE Law and Defamation

- Under Federal Decree Law No. 5 of 2012 on Combatting Cybercrimes (updated 2021), online defamation is a criminal offence in the UAE.
- Defamation is defined as making or sharing false, insulting, offensive, or damaging statements about a person or institution, regardless of whether the statement is true.
- Punishments under UAE law may include fines, imprisonment, and deportation for serious offences.
- Posts, comments, photos, voice notes, or even emojis can be considered defamatory if they cause harm to another person's reputation.

Expectations for Students

- Students must not post, share, or forward inappropriate, offensive, or disrespectful content about peers, teachers, or the school.
- Any group chats created by students (e.g., on WhatsApp, Snapchat, Instagram, TikTok) must remain respectful and free of bullying, gossip, or inappropriate sharing of images/videos.
- Taking photos, recording videos, or posting images of other students or staff without explicit consent is strictly prohibited.

Expectations for Parents

- Parents must raise concerns about the school through official communication channels (email, parent meetings, direct contact with leadership), not through social media posts.
- Parents should avoid posting negative comments about the school, staff, or students on community groups, WhatsApp groups, or social platforms.
- Parents are encouraged to monitor their children's online activities, ensuring respectful and safe use of technology.

Expectations for Staff

- Staff must maintain professionalism on all digital platforms, including personal accounts.
- Teachers must not discuss confidential school matters, students, or colleagues online.
- Staff may not share images of students without written consent from parents and school leadership.

Consequences for Misuse

Any breach of this section may result in:

- For Students: loss of ICT privileges, disciplinary sanctions (detentions, suspensions, exclusions), or escalation to authorities if UAE law is breached.
- For Parents: withdrawal of communication privileges (e.g., restricted access to WhatsApp class groups), meetings with leadership, or referral to KHDA/legal authorities.
- For Staff: disciplinary warnings, suspension, or termination of employment in line with UAE labour law and KHDA regulations.

Positive Use of Social Media

- Students are encouraged to use social media to celebrate learning, showcase creativity, and connect positively with peers.
- Parents are welcome to share their child's achievements, provided they respect the privacy and dignity of other students and staff.
- The school may use official accounts to communicate news, share student achievements, and engage with the wider community in a safe and respectful way.

5. Digital Wellbeing and Electronic Addiction Policy

Purpose

This policy aims to safeguard the wellbeing of students by promoting a balanced and responsible use of digital technology. It sets clear expectations to prevent electronic addiction, reduce the risks of overexposure to screens, and help students develop healthy digital habits that support learning, social interaction, and emotional health.

Scope

This policy applies to all students, teachers, staff, and parents at ASIES. It governs the use of digital devices during school hours and provides guidance for healthy practices at home.

Policy Statement

At ASIES, we recognise that digital devices are powerful tools for education, communication, and creativity. However, excessive or inappropriate use can negatively

impact physical health, emotional wellbeing, academic performance, and social relationships.

We are committed to:

- Encouraging balanced digital use that enhances learning.
- Preventing dependency on devices, gaming, or social media.
- Raising awareness of the signs of electronic addiction.
- Supporting students, staff, and parents with practical strategies to ensure wellbeing in a digital age.

Signs of Electronic Addiction

The school recognises the following as potential indicators of unhealthy digital use:

- Inability to control screen time or excessive preoccupation with devices.
- Withdrawal symptoms when access to devices is limited.
- Decline in academic performance or loss of interest in non-digital activities.
- Fatigue, lack of sleep, or physical strain due to overuse.
- Social isolation, irritability, or neglect of responsibilities.

Guidelines for Digital Wellbeing

In School

- **Restricted Device Use**: Personal devices may only be used for approved educational purposes under teacher supervision.
- **Screen Time Balance**: Lessons integrate screen-free activities to encourage writing, group work, and face-to-face communication.
- **Break and Lunchtime**: Device-free zones encourage physical activity, play, and social interaction.
- **Mindful Use**: Students are reminded to take regular eye and movement breaks during device use.

At Home (Parental Guidance)

- Encourage structured routines with limits on recreational screen time.
- Designate device-free times (e.g., meals, one hour before bedtime).
- Model balanced digital habits as parents/guardians.
- Use parental controls to restrict harmful or time-wasting applications.
- Support children in engaging with hobbies, sports, and family activities beyond screens.

Digital Balance in Learning

- Teachers plan lessons that mix digital and traditional approaches.
- Students are encouraged to use technology as a tool for creativity and problem-solving, not just consumption.
- Parents and teachers work together to ensure children maintain a healthy balance of online and offline learning.

Support and Intervention

- **Awareness Campaigns**: Assemblies, Awareness days, and parent workshops on digital wellbeing.
- **Early Intervention**: Teachers and parents to monitor behaviour; concerning patterns reported to the pastoral and wellbeing team.
- **Counselling**: Students showing signs of addiction will be referred to the school counsellor for guidance.
- **Restorative Action**: If misuse is identified, digital privileges may be temporarily limited while strategies for healthier use are put in place.

Roles and Responsibilities

Teachers

- Model balanced digital use in lessons.
- Educate students about healthy habits, including eye safety, posture, and screen breaks.
- Monitor for signs of digital dependency and report concerns.

Students

- Follow school guidelines for appropriate digital use.
- Engage in offline activities during breaks.
- Report if they or peers are struggling with unhealthy use of devices.

Parents

- Reinforce school expectations at home.
- Monitor children's device usage, including late-night screen use.
- Seek support from school if addiction behaviours emerge.

School Leadership

- Provide training for staff on recognising and addressing digital addiction.
- Ensure ongoing review of this policy in light of new research and community feedback.
- Promote partnerships with external wellbeing experts where needed.

Consequences

If students are found to be excessively misusing devices in ways that impact their wellbeing or academic progress:

- Devices may be temporarily confiscated.
- Parents will be informed and involved in creating a balanced plan.
- Repeated or severe cases may lead to restrictions on BYOD use or additional pastoral interventions.

6. Use of Digital and Video Images Policy

Purpose

This policy ensures that digital and video images of students, staff, and the wider school community are captured, stored, and shared responsibly. It safeguards privacy, protects children from potential misuse of images, and upholds the school's values and compliance with UAE law.

Scope

This policy applies to:

- All staff, students, parents, visitors, contractors, and volunteers who may capture or share images on the school premises or during school activities.
- All formats of images, including photographs, video recordings, live streams, and screen captures, whether taken on personal devices or school-owned equipment.

Principles

1. Respect and Safeguarding – Every child has the right to feel safe and protected. Images must never cause embarrassment, distress, or put students at risk.
2. Consent – Images must only be taken and used with proper consent from parents/guardians and, where appropriate, students.
3. Educational Purpose – Images must only be used for legitimate school purposes such as teaching, learning, displays, school publications, website, and social media (official channels only).
4. Privacy – Images must not reveal sensitive personal information (e.g., full names, addresses, contact details).
5. UAE Law Compliance – Recording or publishing images of individuals without consent may constitute a breach of Federal Law No. 5 of 2012 on Cybercrimes.

Guidelines

Staff

- Always use school-owned cameras or devices when taking photographs or video recordings of students for school purposes.
- Do not store student images on personal devices, personal email, or cloud accounts. Images must be stored securely on school systems.
- When publishing images (e.g., in newsletters, school website, social media), ensure that:

    - Students are appropriately dressed.
    - Images are positive and celebrate achievement.
    - Where possible, only first names are used and no personal contact details are published.
- Staff must not take or share images of students on personal social media accounts.
- Live-streaming or video conferencing must follow safeguarding protocols (appropriate dress, neutral background, and consent in place).

Parents and Visitors

- Parents may only take photos or videos of their own child during school events where permission is given by the school.
- Parents must not post images or videos of other children on social media without explicit consent from those children's parents.
- Recording or photographing staff members without consent is strictly prohibited.
- The school reserves the right to request deletion of any image that breaches this policy.

Students

- Students must not take photos or videos of staff or other students without permission.
- Students must not post or share school-related images on social media without approval.
- Students using devices for learning (BYOD) must only capture images when instructed by a teacher for educational purposes.

Storage and Retention

- Digital images will be stored securely on school servers and accessed only by authorised staff.
- Images will be retained only for as long as necessary for the purpose for which they were taken.
- At the end of the retention period, images will be securely deleted.

Breaches of Policy

- Any misuse of images by staff, students, or parents will be treated as a safeguarding issue.
- Consequences may include removal of ICT privileges, disciplinary action, withdrawal of access to events, or escalation to KHDA/police where UAE law is breached.

Monitoring and Review

- This policy will be reviewed annually alongside the school's child protection and Safeguarding policy.
- Parents will be reminded of this policy at the start of each academic year.

Approval and Sign-Off:
Approved by: Ms. Sadia Wajid
Signature: [Insert Signature]

Date: August 2025

Review Date:
August 2026

Al Sadiq Islamic English School

Digital Technology Policy – Student and Parent Acknowledgement

Dear Students and Parents,
At Al Sadiq Islamic English School, we use technology to support learning, creativity, and communication. To keep everyone safe, respectful, and responsible online, all members of our community must follow our Digital Technology Policy.

Please read the points below, then tick the boxes to show you understand and agree

For Students

I will use technology only for learning.	☐
I will keep my password private and never share it.	☐
I will not take photos, videos, or recordings of anyone without permission.	☐
I will be kind and respectful when using technology and never use bad or hurtful words.	☐
I will not use games, chat apps, or social media during school time.	☐
If I see something that makes me uncomfortable, I will tell a teacher straight away.	☐

Name: _____
Signature: _____
Date: _____

For Parents

I will help my child use devices safely and responsibly at home.	☐
I will not post negative or disrespectful comments about the school or staff on social media.	☐
I will only communicate with my child during the school day through official school channels.	☐
I will make sure my child's device is safe, labelled, and free from games, chat apps, or VPNs.	☐
I will work with the school to support safe and balanced use of technology.	☐

Name: _____
Signature: _____
Date: _____

Al Sadiq Islamic English School

Digital Technology Policy – Teacher Acknowledgement

At Al Sadiq Islamic English School, we use technology to support learning, creativity, and communication. To keep everyone safe, respectful, and responsible online, all members of our community must follow our Digital Technology Policy.

Please read the points below, then tick the boxes to show you understand and agree.

For Teachers

I will use school technology only for teaching and professional purposes.	☐
I will model safe, respectful, and balanced use of technology for students.	☐
I will never use personal devices or accounts to communicate with students.	☐
I will not post or share student information or images without permission.	☐
I will monitor student use of devices in lessons and help them follow safe online practices.	☐
I will report any misuse or unsafe behaviour to the school leadership team.	☐

Name: _____Signature: _____ Date: _____

Approval

- **Approved by:** Principal
- **Date:** August 2025
- **Review:** August 2026