GEMS
مدرسة جيمس الخليج الدولية
Al Khaleej International School

GEMS AKIS SCHOOL POLICIES

E-Policy

Aim and Purpose:

To regulate the behavior of students when they are using all forms of electronic devices and internet connections on the school campus and off the school campus when it is directly and/or indirectly related or linked to any other student, teacher, parent, and/or another staff member at AKIS. This policy will also define the roles and responsibilities of individuals who are involved in all E-safety matters in school.

AKIS will deal with any E-safety incidents and associated behavior as per the behavior and anti-bullying policies and will, where known, inform parents/caregivers of incidents of inappropriate e-safety behavior that take place in or out of school.

Roles and Responsibilities

This policy applies to all members of the school including staff, students, parents/caregivers, and visitors who have access to and are users of school internet connections and devices. The roles and responsibilities are defined for each group as follows:

IT Systems and Network Administrator

- The school internet access must include effective and efficient filtering appropriate for all age groups.
- The ICT system's capacity and security will be reviewed regularly.
- Virus protection is installed, and updated regularly.
- Only approved websites will be accessible.
- List of all accessed websites and online searches will be sent regularly to the Designated Safeguarding Lead and deputies
- All forms of online activities in the school are regularly monitored and any detected misuse is to be communicated to the SLT

Senior Leadership Team:

- SLTs are responsible for the approval of the E- Policy and for reviewing the contents and the effectiveness of the policy
- Regular meetings with the health and safety team, teacher, and parents to discuss the E-policy
- Regular monitoring of e-safety incident logs by liaising with the IT department
- The SLT should ensure that all relevant staff members receive suitable training to enable them to carry out their e-safety roles

All staff members:

- All staff members must be fully aware of the contents of this policy and refer to it regularly
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff who manage filtering systems or monitor ICT will report all cases of misuse or suspected misuse to the relevant SLT member.
- All staff may only use approved school e-mail accounts for school E-communication

Teachers and Teacher Assistants:

- Students will be taught the essentials of internet safety via advisory time, assemblies and campaigns
- Students will be educated in the effective use of the internet in research, including the skills of information location, retrieval, and evaluation.
- Teachers should ensure that the use of internet-derived materials by teachers and students complies with plagiarism and copyright law.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Any suspected misuse must be reported to the phase Principal/Assistant Principal
- Teachers and TAs will monitor the use of devices and device cameras in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- Teachers are aware that all searches and online activity will be closely monitored by the school
- When planning lessons, teachers should check that all websites/links/videos are suitable and appropriate for student use
- When using YouTube links in lessons, teachers must follow the below steps:

    1. Copy the YouTube link that you have chosen for your lesson
    2. Go to the following link: https://video.link/
    3. Copy your YouTube link to generate your Video link box
    4. Copy the safe URL and use it on your plans and power points.

Designated Safeguarding Lead and deputy leads:

Should be trained in all e-safety matters and be aware of the potential for serious child protection/safeguarding issues to arise from:

• Sharing of personal data
• Access to illegal/inappropriate materials
• Inappropriate online contact with adults/strangers
• Potential or actual incidents of grooming
• Cyber-bullying

For all other safeguarding-related E-safety matters, please refer to the GEMS Safeguarding Policy Manual.

Students:

- May only use approved school e-mail accounts for school E-communication and learning
- Must immediately tell a teacher if they receive an offensive e-mail.
- Students are mindful that network and internet use is monitored.
- Must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Are responsible for using their devices in accordance with the BYOD/iPad distribution and behavior policy. This includes their use of digital cameras.
- Have a good understanding of research skills and the need to avoid plagiarism and respect copyright laws
- Must report any abuse, misuse or access to inappropriate materials to their teacher or to a member of the health and safety team and/or the safeguarding team
- Should understand that the school's E-Safety Policy also covers cyberbullying and their actions out of school, if related to any member of the school community

Parents/Caregivers:

Parents/Caregivers play a crucial role in ensuring that their children understand the importance of E-safety practices both in and out of school. The school will take every opportunity to help parents understand these issues through parents' coffee mornings, newsletters, and sharing of school policies. Parents/caregivers' roles and responsibilities include:

- Reading and discussing this E-policy with their children
- Monitor their children's activity on their devices at home
- Report any cases of misuse and/or cyberbullying targeting any member of the school community to a member of the Senior Leadership Team or Health and Safety Team.

Policy Statements

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed or any consequences of internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Health and Safety Team.
- Any complaint about staff misuse must be referred to the school Principal.
- Complaints of a child protection nature must be dealt with in accordance with the safeguarding policy and handled by the Safeguarding team.
- Students and parents will be informed of whom they can approach to make complaints regarding e-safety via assemblies, advisory time, newsletters, and school campaigns.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are strictly forbidden in school. Sending abusive or inappropriate text messages and/or other forms of online messaging/posts will be dealt with in accordance with the AKIS behavior policy.

E -policy Communication with Parents:

- Parents' attention will be drawn to the School e-Safety Policy during the various informational coffee mornings, newsletters, and handbook.
- Parents will, from time to time, be provided with additional information on e-safety.

Cyberbullying

- All students are made aware of the impact of cyberbullying and the ways it differs from other bullying - including the risks of misinterpretation of comments posted. This is communicated to students through assemblies, constant reminders by teachers, and internet safety campaigns.

- AKIS takes all reasonable steps to block access to unsuitable internet sites, including social networking sites, chat rooms, and individual website owners/forums and message board hosts. AKIS has control of the filter and so is able to respond immediately in case of any concerns.

- AKIS is able to conduct a search of internet use records and act accordingly to stop misuse of school equipment and systems.

- Staff is required to keep a record of all bullying cases as evidence and the police can be involved, when needed, to enable the service provider to look into the data of another user.

- Students are made aware that some cyberbullying activities could be criminal offenses. Internet safety day is celebrated and campaigns are held to create awareness for both students and parents.

- AKIS reinforces statutory guidelines about the use of social network sites e.g. Facebook, Twitter, Instagram, and Snapchat.

Online safety – Extract from the GEMS Safeguarding Manual

The School provides internet and intranet access and an email system to students and staff as well as access to other online platforms such as Razkids, IXL, BrainPop, etc. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Manager and his/her team.
Students and staff require individual user names and passwords to access the School's internet and intranet sites and email system which must not be disclosed to any other person. Any student or member of staff who has a problem with their user names or passwords must report it to the IT Department immediately.
No laptop, tablet, or other mobile electronic device may be connected to the School network without the consent of the IT Manager. All devices connected to the School's network should have current and up-to-date anti-virus software installed and have the latest OS updates applied. The use of any device connected to the School's network will be logged in and monitored by the IT Support Department.
The School has a separate Wi-Fi connection available for use by visitors to the School. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.
All incidents of youth-produced sexual imagery (YPSI) will be dealt with as safeguarding concerns. The primary concern at all times will be the welfare and protection of the young people involved. Students who share sexual images of themselves or their peers are breaking the law. However, the school believes it is important to avoid criminalizing young people unnecessarily. The school will therefore work in partnership with parents and external agencies with a view to responding proportionately to the circumstances of any incident.
All incidents of YPSI must be reported to the DSL as with all other safeguarding issues and concerns. Staff will not make their own judgments about whether an issue relating to YPSI is more or less serious enough to warrant a report to the DSL. If, at any point in the process, there is concern that a young person has been harmed or is at risk of harm, a referral will be made to the relevant agency.

Appendix 1 – B.Y.O.D Policy

Al Khaleej International School "Bring Your Own Device" (B.Y.O.D.) September 2015
Policy and responsible use guidelines – Reviewed December 2022

Purpose:

Al Khaleej International School uses instructional technology as one way of enhancing our mission to teach the skills, knowledge, and behaviors students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity, and critical thinking in a variety of ways throughout the school day. In an effort to increase access to those 21st Century skills, AKIS allows personal devices on our network and school grounds for grades 9-12 students who follow the responsibilities stated in this policy and guidelines regarding B.Y.O.D. The use of personal devices by students is mandatory, and all grade 9-12 students must read, sign and adhere to this BYOD agreement. An important component of B.Y.O.D. will be educated about appropriate online behaviors. We will review cyber-safety rules with students frequently throughout the course of the school year and will offer reminders and reinforcement about safe online behaviors. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal devices. The use of technology is not a necessity but a privilege. When abused, privileges will be taken away.

Device Types:

For the purpose of this program, the word "devices" will include laptops, netbooks, iPods, iPads, tablets, and e-Readers. Please note that Nintendo DS (and/or other gaming devices with internet access, and mobile and smartphones including the iPhone and Samsung Galaxy phones are not permissible.

Guidelines:

- Students and parents/guardians participating in B.Y.O.D. must adhere to the Parent/Student agreement which is in the school agenda, this policy, and any other related policies. Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects.
- Approved devices must be in silent mode while on the school campus unless otherwise allowed by a teacher.
- Headphones may be used with the teacher's permission.
- Devices may not be used to cheat on assignments, quizzes, or tests or for non-instructional purposes.
- Students may not use devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities, unless otherwise allowed by a teacher.
- Any photo/video involving any member of the school community can only be posted with the express written permission of the concerned teacher and Principal.
- Devices may only be used to access computer files on internet sites that are relevant to the classroom curriculum.
- Printing from personal devices will not be possible at school.
- Personal devices must be charged prior to school and run on battery power while at school. Charging of devices will not be permitted at AKNS.
- Students are not permitted to:

1. Bring a device on premises that infect the network with a virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information.
2. Process or access information on school property related to "hacking." Altering or bypassing network security policies.

Students and Parents/Guardians acknowledge that:

The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited. AKIS is authorized to collect and examine any device that is suspected of causing technology problems or was the source of an attack or virus infection, with parental permission.

An important point to note:

Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the student code of conduct or this agreement. If the device is locked or password protected, the student will be required to unlock the device at the request of a school administrator. Parent permission will be requested before this is done.

Lost, Stolen, or Damaged Devices:

Each user is responsible for his/her own device and should use it responsibly and appropriately. AKIS takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices. Please check with your homeowner's policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.

Usage Charges:

AKIS is not responsible for any possible device charges to your account that might be incurred during approved school-related use.

Network Considerations:

Users should strive to maintain appropriate bandwidth for school-related work and communications. All users will use the "GEMS-BYOD" wireless network to access the internet. AKIS does not guarantee connectivity or the quality of the connection with personal devices. AKIS IT department is not responsible for maintaining or troubleshooting student tech devices.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or device privileges as well as other disciplinary action. During the course of the school year, additional rules regarding the use of personal devices may be added.

Student Name: _____ Student Signature: _____
Grade and section: _____

Parent/Guardian Signature: _____ Date: _____
Assistant Principal Signature: _____ Date: _____
IT Department Staff Member Signature: _____ Date: _____

Appendix 2 – iPad Distribution Policy

SOP (Standard Operation Procedure) steps	Time frame
IT department orders iPads based on the requirements submitted by the Elementary team.	The first week of July
IT department updates the iPads to the latest iOS.	-Existing iPads: first week of July -New iPads: first week of August
IT Department installs all required Apps and adds them to folders based on the KG and Elementary teams' requests.	
IT department will label each iPad and charger with the student's name and grade level, iPad contract, and the unique serial number (with all iPad specifications and details) will be attached to each iPad.	The first week of August
IT department will label iPad' trolleys (Trolleys 1, 2, 3, etc …) with iPad details and students' names at the top of each trolley.	
Accounts to send a list of students who paid for the iPads to the Head of Technology.	-Initial list: last week of August - Ongoing lists: according to payments
IT department to share with homeroom teachers copies of the iPad agreement who, in turn, will distribute them to the students who have paid.	Immediately after payment
Homeroom teachers hand the iPads to those who return the contract only. KG2-5 students will be allowed to take the iPads home only after they settle (to be decided by the admin team) to go over the rules and reminders at school. KG1 students will use their iPads in school only	Immediately after receiving the contract.
Head of Technology to send instructions to the KG and Elementary team to communicate with parents how and when to return the iPads.	Early June Suggestion (Last week of May)
Teachers are to provide a list of students who did not return the iPads to the IT & Technology Department copying the principals and Assistant Principals.	Last week of June
Homeroom teacher and Technology Department to follow up with the students who did not return the iPads.	Last week of June
Parents will be charged for damaged iPads or iPads not returned (as per the contract sent to parents). The list needs to be provided to Accounts in an excel format with Full Student ID, Full Student Name (as per school records), Grade and Section.	Last week of June

EDUCATION

Reviewed by: SLT
Reviewed on: Dec 2022