


Ras Al Khaimah American Academy				
<b>Subject:</b> Student Acceptable Use Policy (AUP) & Technology Usage Agreement			<b>SOP No:</b> RAKAA-IT-09	<b>Controlled Copy No:</b>
			<b>Revision No:</b> 04	
<b>Written by:</b>	<b>ICT Manager</b> Asma Odawa	<b>Date:</b> Feb 17, 2014	<b>Based on:</b> Common practice	
<b>Amended and improved by:</b>	<b>Assistant Online Safety Lead</b> Katrina Scotford	<b>Date:</b> April 30, 2022	<b>Supersedes:</b> Feb 17, 2014	<b>Issued on:</b> May 17, 2022
<b>Approved by:</b>	<b>Principal</b> Sandra Zaher	<b>Date:</b> May 18, 2022	<b>Distributed to:</b> Principal (Original)	<b>Pages:</b> 19
<b>Authorized by:</b>	<b>Principal</b> Sandra Zaher 	<b>Date:</b> May 18, 2022	<b>Effective as of:</b>	
			<b>Review date:</b>	

## Contents

Introduction	2
Personal Safety	2
Security Systems	3
Personal Devices	4
Software, Hardware, and File Sharing	5
E-mail and Messages	6
Plagiarism and Copyright	7
Privacy	7
Access to the RAKAA network	8
General and Best Practice	8
Warning	9
Definitions	9
References	11
RAKAA Online Safety Group	11
Students and Parents Acceptable Use Agreement Forms	12

## **Introduction**

This policy aims to inform all students and parents at RAKAA of what is considered as acceptable use of the RAKAA network and school devices. It also identifies what would be regarded as unacceptable use and provides guidance on what will happen should any users breach the acceptable use policy terms. This policy will not cover every aspect of electronic device use, but it does address many of the major matters. We are trying in this policy to provide the general expectations of how to use electronic devices in a safe, responsible and appropriate manner. The use of technology to provide educational material is a privilege for any student who is willing to be responsible and abide by the guidelines set in this document.

## **This Acceptable Use Policy Agreement is intended to ensure:**

- ✓ That students in our care at RAKAA will be responsible users who can stay safe while using the internet and other digital technologies for educational, personal, and recreational use.
- ✓ That RAKAA school network, systems, and students are protected from acts of misuse, whether accidental or deliberate, that could put the security of the systems at risk
- ✓ That any student who knowingly or willingly attempts to access any prohibited information or websites or breaks any conditions will be subject to disciplinary sanctions.

## **Personal Safety**

- ✓ Technology continues to develop at an ever-increasing rate, and as it does, the risks to our personal safety when using the internet grow too. At RAKAA, we stress the importance of being very cautious about who you choose to share your personal details with when you are online. Students must never reveal their full name, home address, mobile phone number, or e-mail address to anyone who is a stranger to them.
- ✓ Students must always inform their teacher or a trusted adult if they receive any messages from unknown sources or if they have visited any websites that may

include inappropriate language or any pictures, videos, or other content that makes them uncomfortable.

- ✓ Students are made aware of the importance of being themselves online. They should not pretend to be anyone else.
- ✓ Students are regularly reminded that they must not arrange to meet up with anyone they have met online.
- ✓ If students have any doubts about content they have accessed online, they must ensure that they ask an appropriate adult to review it.

### **Security Systems**

- ✓ To keep all students safe when accessing content online, the school has put in specific access procedures based on the age level of the students. That includes the assignment of students' passwords.
- ✓ Students must only access the RAKAA network using Students Wi-Fi credentials. This network has firewalls to prevent students from accessing any website the school's E-Safety team has deemed inappropriate.
- ✓ Students must not attempt to go beyond the areas they have been granted access to; this includes:
  - Using VPNs, Ultra Surf, Hotspot, or any other program which serve the same purpose
  - Trying to bypass school's firewalls.
- ✓ Any student attempting to log on to the RAKAA Teacher's Network or any other network not assigned to them risks losing access to the RAKAA network and other serious sanctions following the school's Code of Conduct.
- ✓ All students MUST only use the school's network to access the internet while on-site. All use of mobile data is prohibited and considered a breach of the school's Acceptable Use Policy.
- ✓ Students at RAKAA are granted access to different websites and platforms using passwords assigned by the school. No student is to share their password or username with any other student, and all students must log out of websites or RAKAA devices when finished. If another student accesses a website or computer

while logged in as you and does something wrong, you might be held responsible for their actions.

- ✓ If you suspect that another student might know your password, then contact your teacher, the IT department, or a member of the Online Safety Team and request help in changing your password immediately.

### **Personal Devices**

- ✓ Personal devices include laptops, tablets, Chromebooks, mobile phones, and MacBooks.
- ✓ Students should not use mobile phones while in school. Students are prohibited from having mobile phones in class and must turn them in to a nominated adult each morning.
- ✓ Personal devices may only be used when a teacher has given permission and then can only be used for educational purposes. It should not be used for games, chat, or entertainment.
- ✓ Students may not use their personal devices during break times while waiting to be dismissed or on school transport.
- ✓ The use of mobile data to access the internet by any student at RAKAA is prohibited as this cannot be monitored or controlled through school's firewall.
- ✓ Students are not permitted to take photos or videos while in school on any of their personal devices without the express permission of a member of staff. No student is permitted to take photos of anyone else without their permission.
- ✓ Features on personal devices such as Airdrop or Bluetooth must be switched off when on-campus. Bluetooth may only be used for headsets and must only be with a teacher's permission.
- ✓ Although we take great care to maintain the safety of everyone and their belongings while at RAKAA, the safety and security of your personal devices is your own responsibility. You are responsible for ensuring that you have placed your device in your backpack at the end of each day. RAKAA assumes no responsibility or financial liability for any damage the students or parents suffer, including but not limited to theft, physical damage, loss of data or software, or malfunctions of the personal device. If a device appears to have been stolen, the student involved must

immediately inform an ICT Manager. Most of the devices have a device locator. We recommend the student to enable this feature if possible. It is always a good idea to record the device's serial number in case of theft.

- ✓ Your personal device must be fully charged each evening, ready to bring to school with you the following day. The school will not provide chargers or outlets to charge devices. Students must bring their own power banks in to charge their devices on-site.
- ✓ The use of personal devices must not interfere with or distract the learning environment.
- ✓ Students must surrender their personal devices to any teacher or administrator upon request and grant this authorized personnel permission to examine their system to establish whether any policies have been violated. When personal device is brought to school students should not expect privacy as to any data saved in their devices.
- ✓ Technical support for a student's personal device will not be provided. It is the student's responsibility to care for his/her own device and keep it in good working order. Students who are facing technical issues in their personal device will need to take care of the issue out of the classroom and immediately.
- ✓ The AUP may be amended from time to time.
- ✓ Students will not attempt to gain access to any electronic device for which they are not authorized, or for which they do not own.

### **Software, Hardware, and File Sharing**

- ✓ Students at RAKAA must not attempt to download any programs from the internet onto the school network or devices.
- ✓ Students will not attempt to delete data in school's devices. All students will immediately report to ICT teacher or the IT department if there is any indication that any data has been tampered with or deleted.
- ✓ Students will not tamper with other student's work or the proper use of electronic devices at all times.
- ✓ Students are strictly prohibited from using peer-to-peer networks, file-sharing programs, Airdrop, or Bluetooth, Network password revealer, telnet/ssh, or

messenger programs as well as other resource intensive applications (e.g., Kazaa, LimeWire, etc.) at RAKAA. Using network monitoring software is considered a serious offense of the AUP and will result in disciplinary action, up to and including immediate expulsion from RAKAA. Access to the RAKAA school network is considered a privilege, and it can be revoked for any reason at the discretion of the school administration and the ICT Manager.

- ✓ Any damage or problems noticed on the RAKAA network, applications or school devices must immediately be reported to the IT department or a suitable adult.
- ✓ Any school devices must be left in their designated place. If peripherals such as headphones are borrowed, the IT department or IT teacher must be informed, and consent given.
- ✓ Only the IT department may move, repair, reconfigure or modify any of the devices at RAKAA.
- ✓ If there is an application which is considered unsuitable, (this will be decided by the IT department) it must be uninstalled from the device.

### **E-mail and messages**

- ✓ All students should ensure that they check their e-mail messages regularly and respond to messages promptly.
- ✓ Please ensure that you do not reply to spam messages or e-mails, as this will create more spam on the network. Delete any spam messages straight away and inform the IT department for assistance.
- ✓ Users must make sure that they do not open an attachment from an unknown source as it may contain a virus that can cause severe damage to the RAKAA network.
- ✓ Students must not use their e-mail accounts during classes unless given express permission by their teachers.
- ✓ No student should send or forward any unnecessary messages or messages that do not pertain to education to a large number of people.
- ✓ Students sharing messages using Microsoft TEAMS platform must ensure that the content is polite and relevant to educational purposes.

### **Plagiarism and Copyright**

- ✓ At RAKAA, we take plagiarism and copyright seriously, and we regularly remind the students of their responsibility to avoid plagiarising the work of others. Students are taught that plagiarism involves claiming ideas, written work, or any content produced by others and shared online and presenting it as their own original work. Students are required to check that their work is original and that they have cited any sources they have used.
- ✓ Copyright involves reproducing a piece of work without the creator's consent. To avoid breaking copyright laws, students should ensure that they have requested the copyright owner's permission before recreating their work in a different manner.
- ✓ Content copied from E-Textbooks must be cited. Students must appreciate that content in E-Textbooks is copyrighted, and it is their responsibility to avoid breaking the copyright laws.

### **Privacy**

- ✓ Any files, e-mails, or content on the system are the property of RAKAA. As a result, system administrators and staff have a right to access them as and when required.
- ✓ Never assume that any e-mail sent online is entirely secure. If you are sending sensitive information via e-mail, please ensure that the documents being sent are password-protected to protect the data.
- ✓ All access to the RAKAA network and school devices is monitored, as are messages sent using the school assigned e-mail address and Microsoft Teams.
- ✓ If you are suspected of breaching the AUP that you have signed, then your own personal device can be searched by the ICT Manager.
- ✓ To continue maintaining the safety and security of the RAKAA network and its reputation within the community, the school reserves the right to search the internet for inappropriate material that any RAKAA student posts on social media sites.

### Access to the RAKAA network

- ✓ Students and parents/carers must sign the Acceptable Use Policy to be granted access to the RAKAA Student Network.
- ✓ Students are requested to provide the school IT department with their Personal Device's MAC (Media Access Control) Address/Physical Address for security reasons. Failure to provide this information will result in access to the network being denied.
- ✓ Students can connect ONLY using the school's wireless network after the completion of the registration procedure when the student's device is connecting for the first time to the wireless network. All usage must be in accordance with the terms of the Internet Agreement.
- ✓ Students must only access the RAKAA Student network. They must not be granted access to any other network. If anyone suspects that they have accessed a network which they are not supposed to, it must be reported to a member of the IT department.

### General and Best Practice

- ✓ Students must ensure that they use their own good judgment when interacting online. They must be aware that whatever they post online is there forever, so they must ensure that they always think before they post.
- ✓ Whenever a student has finished using a school device, they must ensure that they log off when they have finished.
- ✓ All students must ensure that they regularly save their work and back it up on their school's One Drive account.
- ✓ All students need to ensure that they follow Health and Safety Guidelines when using devices and make sure that they look away from their device screens every 10 minutes to rest their eyes. Users must ensure that the chair they are using while on their devices is of a suitable height compared to the desk and that they are sitting in the correct position.
- ✓ All students should ensure that they regularly clear out their e-mail accounts by deleting any unnecessary messages and free up storage space.



- ✓ If in doubt about anything on the RAKAA network or school devices, students should seek advice from the IT department or a member of the E-Safety team.

### **Warning**

- ✓ Any student that is suspected of breaching the AUPs they have signed will be referred to the principal, who is the Online Safety Lead, and she will decide upon the course of action to be taken in line with the RAKAA Code of Conduct.

### **Definitions**

- **RAKAA Network**

The school provided a network for students to log on to and access the internet. Students may only access the dedicated RAKAA Student Network using their credentials. RAKAA network has comprehensive filtering systems to prevent access to any unsuitable websites or content.

- **RAKAA Devices**

Any digital device including desktop computers, laptops, tablets, electronic equipment, and active panels.

- **School approved communication channels**

The only school-approved communication channels are Microsoft Teams, school-assigned e-mail accounts, and Seesaw for limited classes, and any other platform that has been approved by SLT for the school community.

- **Personal Devices**

Any device brought in by a student that is granted access to the RAKAA network, including mobile phones, tablets, Chromebooks, and laptops. Students must abide by the rules in this policy to bring their personal devices to school.

- **Storage Devices**

Any device used to store and transfer data from one device to another. No student at RAKAA is permitted to use a USB or other storage device on any RAKAA device. If content or files need to be shared, they must be sent electronically via e-mail, cloud sharing on the OneDrive, or via the school-designated platform Microsoft TEAMS.

- **File sharing**

Sharing of content using Airdrop, Bluetooth, or any other wireless transmission is prohibited at RAKAA. As stated above, the only accepted ways of sharing data are via the school-designated e-mail address or using Microsoft Teams.

- **Plagiarism**

Intentionally copying or using someone else's work as your own without citing where you found the information. Plagiarism is strictly prohibited at RAKAA and will be dealt with according to the school's Code of Conduct.

- **Copyright**

The exclusive and legal right of a person who creates content for the purpose of sharing with others. Breaches of copyright are not tolerated at RAKAA and will be dealt with according to the school's Code of Conduct.

- **E-Textbooks**

Much of the curriculum provided at RAKAA contains access to E-textbooks. An E-textbook is an electronic textbook. They are electronic versions of the textbooks that have been issued to the students and often contain interactive activities as well.

- **Citation – Cite**

When referring to a quote, paragraph, or any content created by another for purposes of evidence in an assignment or piece of work, students, or any other document creators must include details of where they found the content. This is known as citing their sources.

- **Harassment**

Harassment means to act towards another person consistently and persistently in a way that causes distress or annoyance to them. This includes sending unwanted and rude messages online and posting images of others that may cause them distress.

- **Cyberbullying**

The increase of social media platforms in the past decade has directly impacted the cases of cyberbullying experienced by many students worldwide. Cyberbullying is the use of any electronic communication, whether it is posted on social media, e-mail messages, messages sent through apps such as WhatsApp, or sharing of videos or

pictures that may cause embarrassment or humiliation to another person. It also includes sharing negative, harmful, or mean content about other people. (See RAKAA's Anti-bullying policy for more details).

### **References:**

- [Student Email Communication Policy](#)
- [Filtering Policy](#)
- [Anti-bullying Policy](#)
- [Parent Privacy Policy](#)
- [Internet Agreement](#)
- Social Media Policy
- Online Safety Policy
- [Password Policy and Guidelines](#)
- [Devices Use Guidelines](#)

### **RAKAA Online Safety Group**

- Dr. Sandra Zaher – Online Safety Leader
- Ms. Katrina Scotford – Online Safety Lead Assistant
- Mrs. Farhat Riffat – Online Safety Lead Assistant
- Ms. Asma Odawa – ICT Manager Grades 3-12 Girls
- Mr. Naveed Ahmad – ICT Manager K-2 and Grades 5-9 Boys
- Dr. Maria Monce – Head of Student Support/Academic Advisor
- Mr. Iyad Hamdan – Boys school Counsellor/Academic Advisor

### **RAKAA Grade 6-12 Students Acceptable Use Agreement Form**

This agreement needs to be submitted yearly and will be amended to include important technical information for any device that will be connected to RAKAA network.

Signing this agreement shows that you have read, understood, and agree to the terms and rules of the Student Acceptable Use Policy (AUP) & Technology Usage Agreement and in addition will comply with all class and school rules while using technology. If you do not return a signed agreement to the school, you will not be given access to the school's network.

**As a student who is granted access to the RAKAA network and any school devices I pledge to use technology in the following acceptable ways:**

#### **I WILL:**

- ✓ Only use the RAKAA Student Network with my assigned password.
- ✓ Only use technology, whether a school device or my own personal device for school-related activities at school.
- ✓ Follow the rules in the RAKAA Behaviour Policy and will behave online in the same way as I would behave offline.
- ✓ Treat all resources with care.
- ✓ Report any problems with equipment to a teacher or other adult.
- ✓ Respect the beliefs and views of my fellow students and teachers.
- ✓ Engage in positive, constructive discussions on the school's Microsoft TEAMS platform.
- ✓ Only use IT devices when approved by a teacher for educational purposes.
- ✓ Report any threatening, harmful, or inappropriate images, messages, or posts online to a teacher or responsible adult.
- ✓ Cite my sources for video, pictures, music, or text when researching online.
- ✓ Only share content using the school's Microsoft TEAMS platform or my school-issued email address.
- ✓ Seek support from the IT department if I am unable to access the Student Network.
- ✓ Be cautious online and will take care to protect my personal data and the data of others at RAKAA.

**I understand that if I do not follow the conditions of the Acceptable Use Policy, my access to the RAKAA network may be restricted and I could have disciplinary action taken against me, as outlined in the RAKAA Code of Conduct and Ministry of Education policies.**

Name of Student: .....

Student Signature: .....

Grade: .....

Date: .....

Mac Address/Physical Address of Computing Device(s) - (one per device):

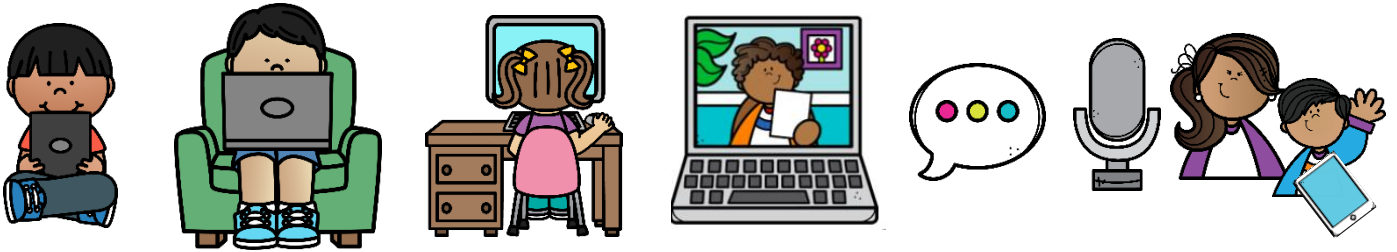
.....  
Description: .....

Example

01:23:45:67:89:AB

Description: Lenovo ThinkPad T480

**RAKAA Grade 1-5 Students Acceptable Use Agreement Form**



At RAKAA we enjoy using technology and know how important it is to our learning. We know that it is important to follow certain rules when using our own devices and the school's devices.

**I agree to follow the rules below when logging on to the RAKAA network or while using any device on campus.**



**Things I will do:**

- ✓ I will only use my personal device or a RAKAA device when my teacher has given me permission to.
- ✓ I will only access sites that my teacher has asked me to visit.
- ✓ I will keep my username and password to myself
- ✓ I will ask my teacher for help if I think that I have accessed something I should not have or if I'm not sure what to do.
- ✓ I will tell my teacher if I discover anything that worries or upsets me on the screen.
- ✓ I will only access the RAKAA network using the password provided for student use.
- ✓ I will only send messages to other students that use kind and respectful words.

**I know that anything I do on the RAKAA network may be monitored by the school on any device.**

**I know that if I break any of these rules, my access to the RAKAA network or use of any device while in school, may be terminated and my parents contacted.**

Name of Student: .....

Student Signature: .....

Grade: .....

Date: .....

Mac Address/Physical Address of Computing Device(s) - (one per device):

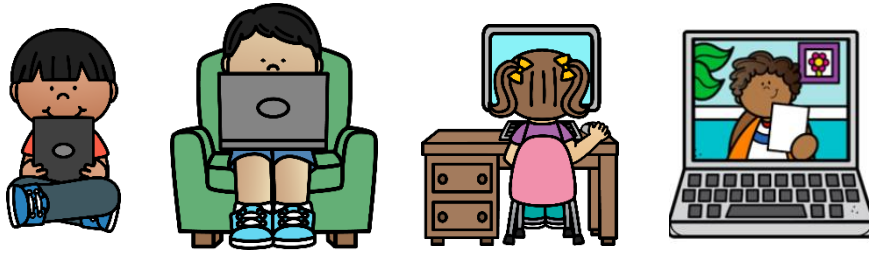
.....  
Description: .....

Example

01:23:45:67:89:AB

Description: Lenovo ThinkPad T480

**RAKAA KG Students Acceptable Use Agreement Form**

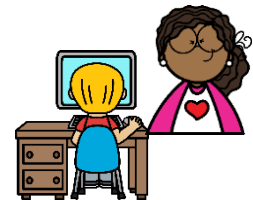


To help me to stay safe online at RAKAA:

Acceptable Use



✓ I will only use a device when a teacher tells me I can.



✓ I will always tell my teacher if I see anything on the computer that makes me unhappy or scared.



✓ I will ask for help from a teacher if I am not sure what to do or think I have done something wrong.



✓ I will only use my own device



✓ I will use kind words online when talking to others.





Name of Student: .....

Student Signature: .....

Grade: .....

Date: .....

Mac Address/Physical Address of Computing Device(s) - (one per device):

.....  
Description: .....

Example

01:23:45:67:89:AB

Description: Lenovo ThinkPad T480

**I have read this policy and discussed it with my child and I agree that they will follow the conditions set out in it.**

### RAKAA Parent/Carer Acceptable Use Agreement

We believe that all our students must have access to technologies to prepare them with the essential skills that they will need to become successful members of our society and valuable workers of the future. We also recognize our responsibility to keep our student safe while online and develop their understanding of what it means to be a genuinely responsible digital citizen.

As a parent or carer, you are expected to sign an individual copy of the Student Acceptable Use Policy (AUP) & Technology Usage Agreement for each child as there are different requirements based upon their age and use of technology.

Parents are requested to read the Acceptable Use Policies sent out for their child's age range and discuss all requirements with their child so that both you and they understand what they are agreeing to.

**As the parent or carer of the child listed in the section above, I hereby give my consent for my child to have access to the internet and any digital technologies whilst onsite at RAKAA.**

I acknowledge that my child's teachers have discussed the RAKAA Student Acceptable Use Policy (AUP) & Technology Usage Agreement with my child and that they are receiving online safety education appropriate to their age group to teach them how to be safe online. I further understand that my child has signed the Student Acceptable Use Policy (AUP) & Technology Usage Agreement and that they will be held fully responsible for all of their actions online.

Whilst at home, I will always encourage my child to adopt safe use of the internet and digital technologies.

I will support the school by monitoring the content on my child's device on a frequent basis. If my child violates any aspect of this agreement, I understand that RAKAA will confiscate the device and that I personally must pick it up directly from an administrator with my child present to discuss the violation.

I hereby grant my permission for the school to record my child's MAC Address on their system.

Finally, I acknowledge and support the monitoring of my child's use of the RAKAA network and digital technologies, and I understand that the school will contact me if they have any

worries or concerns about any possible breaches of the Student Acceptable Use Policy (AUP) & Technology Usage Agreement by my child.

Signing this agreement shows that you have read, understood, and agree to the terms and rules of the Student Acceptable Use Policy (AUP) & Technology Usage Agreement.

Name of the Parent: .....

Signature of Parent/Carer: .....

Date: .....