Ras Al Khaimah American Academy				
Subject: Staff Acceptable Use Policy (AUP) & Technology Usage Agreement			**SOP No:** RAKAA-IT-010	**Controlled Copy No: 2**
			Revision No: 02	
Written by:	**ICT Manager** Asma Odawa	**Date:** August 22, 2021	**Based on:** Current practice	
Checked by:	**Assistant Online Safety Lead** Katrina Scotford	**Date:** May 16, 2022	**Supersedes:** August 22, 2021	**Issued on:** May 20, 2022
Approved by:	**Principal** Sandra Zaher	**Date:** May 20, 2022	**Distributed to:** Principal (Original)	**Pages:** 11
Authorized by:	**Principal** Sandra Zaher 	**Date:** May 20, 2022	**Effective as of:**	
			Review date:	

Contents

Introduction

This policy aims to inform all staff at RAKAA of what is considered as acceptable use of the RAKAA network, school devices and personally owned electronic devices. It also identifies what would be regarded as unacceptable use and provides guidance on what will happen should any staff 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 acceptable manner. The use of technology to provide educational material is a privilege for any staff who is willing to abide by the guidelines set in this document.

This Acceptable Use Policy Agreement is intended to ensure:

- ✓ The staff in our employment 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 staff are protected from acts of misuse, whether accidental or deliberate, that could put the security of the systems at risk
- ✓ That any staff 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. Staff must model best practices while online with the students and ensure they do not share their personal data or any identifying information.
- ✓ If a staff member has any doubt about content they have accessed online, they must ensure that they ask a member of the Online Safety Group or IT department to review it.

- ✓ Staff must have a valid antivirus software installed in their personal devices and it should be kept up to date. Staff need to ensure that they are regularly updating their systems and making a backup for their important files in one drive.
- ✓ Staff must always inform the IT department or a member of the Online Safety Group if they:
    - Received any messages from unknown sources
    - Visited any website that included inappropriate language or pictures, videos, or other content that makes them uncomfortable.
- ✓ Staff can use the following link to report their concerns: https://forms.office.com/r/bhW2thQhAb

Security Systems

- ✓ Staff must only access the RAKAA network using Staff Wi-Fi credentials. This network has firewalls to prevent staff from accessing any website the school's E-Safety team has deemed inappropriate.
- ✓ Staff 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.
- ✓ All staff are fully aware that students may only use the RAKAA Students network and understand that it is against the AUP to give any student access to a different network.
- ✓ Any staff attempting to log on to 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 staff 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.
- ✓ Staff at RAKAA are granted access to different websites and platforms using passwords assigned by the school. No staff is to share their password or username with any student or other colleagues, and all staff must log out of websites or RAKAA

devices when finished. If another staff 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 your account is compromised then contact the IT department immediately to reset your password. If you suspect that a student might know the RAKAA Teachers network password, in that case, you must inform the IT department instantly.

Personal Devices

- ✓ Personal devices include laptops, tablets, Chromebooks, mobile phones, and MacBooks.
- ✓ Staff members are provided with a desktop computer or laptop in their classrooms. However, they are also expected to use their own personal devices to teach remotely and work on school-related documents.
- ✓ Personal devices may only be used for educational and administrative purposes. It should not be used for chat, or entertainment.
- ✓ Staff shouldn't use mobile data to access the internet while in campus as this cannot be monitored or controlled through school's firewall.
- ✓ Features on personal devices such as Airdrop or Bluetooth must be switched off when on-campus. Bluetooth may only be used for connecting devices such as headsets, mice, keyboards, etc..
- ✓ 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. RAKAA assumes no responsibility or financial liability for any damage the staff 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 staff involved must immediately inform an ICT Manager. Most of the devices have a device locator. We recommend the staff to enable this feature if possible.
- ✓ The use of personal devices must not interfere with or distract the learning environment.
- ✓ School will not provide technical support for staff personal devices. Staff members should keep their devices in good working order. Technical issues should be dealt

with promptly. If a staff member is experiencing technical issues in personal device, school will provide a temporary laptop for a week until the issue is resolved.

- ✓ The AUP may be amended from time to time.
- ✓ Staff will not attempt to gain access to any file, account, or electronic device for which they are not authorized, or for which they do not own. In addition, staff will not attempt to modify or destroy data of another staff member.

Software, Hardware, and File Sharing

- ✓ Staff at RAKAA must not attempt to download any program from the internet onto the school devices.
- ✓ Staff will not tamper with other staff's work or the proper use of electronic devices at all times.
- ✓ Staff 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 and will result in disciplinary action. 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.
- ✓ Any school devices must be left in their designated place. If peripherals are required such as headphones, remote controls, interactive pens and printing cards, teachers need to fill and sign the IT requisition form. Received peripherals should be returned by end of academic year in a good working condition.
- ✓ 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 staff 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 contact the IT department for assistance if required.
- ✓ Staff 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.
- ✓ No staff should send or forward any unnecessary messages or messages that do not pertain to education to a large number of people.
- ✓ Staff sharing messages using Microsoft TEAMS platform must ensure that the content is 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. Staff members have a duty to remind students about plagiarism and should model best practices when using other sources in class.
- ✓ Copyright involves reproducing a piece of work without the creator's consent. To avoid breaking copyright laws, staff should ensure that they have requested the copyright owner's permission before recreating their work in a different manner.
- ✓ The reproduction and distribution of copyrighted materials without appropriate authorization is prohibited. Using networks or technology equipment for any illegal activity, including violation of copyright or other laws, is prohibited.

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.

Access to the RAKAA network

- ✓ Staff must sign the Acceptable Use Policy to be granted access to the RAKAA Teachers' Network.
- ✓ Staff 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.
- ✓ Staff can connect ONLY using the school's wireless network after the completion of the registration procedure when the staff's device is connecting for the first time to the wireless network.
- ✓ Staff must only access the RAKAA Teachers' network. They must not be granted access to any other network.
- ✓ Staff will not deliberately distribute or download any material in such a manner that causes congestion of networks.

General and Best Practice

- ✓ All staff must ensure that they adhere to the RAKAA Acceptable Use policy 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 staff has finished using a school device, they must ensure that they logged out from their accounts.
- ✓ All staff must ensure that they regularly save their work and back it up on their school's One Drive account.
- ✓ All staff 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.
- ✓ All staff 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, staff should seek advice from the IT department or a member of the E-Safety team.

Warning

- ✓ Any staff 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 staff to log on to and access the internet. Staff may only access the dedicated RAKAA Staff 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 any other platform that has been approved by SLT for the school community.

- **Personal Devices**

  Any device brought in by a staff that is granted access to the RAKAA network, including mobile phones, tablets, Chromebooks, and laptops. Staff 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 staff 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.

- **Citation – Cite**

  When referring to a quote, paragraph, or any content created by another for purposes of evidence in a piece of work, staff, 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.

References:

- Policy for Use of Removable Media
- Staff Email Communication Policy
- Filtering Policy
- Data Protection Policy
- 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 Staff Support/Academic Advisor
- Mr. Iyad Hamdan – Boys school Counsellor/Academic Advisor

Staff Acceptable Use Policy (AUP) & Technology Usage Agreement Form

By signing this form and turning it in to the ICT Manager you agree to the terms of the Staff Acceptable Use Policy (AUP) & Technology Usage Agreement.

This form must be completed whenever required and must be filled out or modified to include necessary technical information for any device that you wish to use with RAKAA network.

Staff Agreement

I have read, understand, and will abide by the RAKAA Staff Acceptable Use Policy (AUP) & Technology Usage Agreement. I further understand and accept that any violation of the regulations and policies in the agreement is unethical and may result in revocation of my privileges, school disciplinary action, and/or appropriate legal action.

Staff Name: .....

Staff Signature: .....

Date: .....

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

.....

Description: .....

Example

01:23:45:67:89:AB

Description: Lenovo ThinkPad T480