ACCEPTABLE USE POLICY FOR STAFF

Acceptable Use Policy Agreement is intended to ensure:

- That staff in will be responsible users who can stay safe while using the internet and other digital technologies for educational, personal, and recreational use.
- That 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 do, the risks to our personal safety when using the internet grow too. At school, we stress the importance of being very cautious about whom you choose to share your personal details with when you are online. Staff must be the 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 valid antivirus software installed in their personal devices and it should be kept up to date. Staff needs 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 or 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://rakscholars.com/PageContentNew.aspx?id=502

Security Systems.

- Staff must not attempt to go beyond the areas they have been granted access
- All staff is fully aware that students may only use the MS Teams credentials given by the school.
- Any staff attempting to log on to any other network not assigned to them may face 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.
- No staff is to share their password or username with any student or other colleagues, and all staff must log out of websites or 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 contacts the IT department immediately to reset your password. If you suspect that a student might know the school 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 smart board 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 at the school
- 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 school, the safety and security of your personal devices is your own responsibility. School 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.
- 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 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 is strictly prohibited from using peer-to-peer networks, file-sharing programs, Airdrop, or Bluetooth, at school. Using network monitoring software is considered a serious offense and will result in disciplinary action.
- Any damage or problems noticed on the school devices must immediately be reported to the IT department
- If peripherals are required such as headphones, remote controls, interactive pens etc. 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 school
- If there is an application which is considered unsuitable, (this will be decided by the IT department) it must be uninstalled from the device.

UNACCEPTABLE USE

- Staff must always respect the different views and beliefs of students, parents and colleagues.
- Use of rude, indecent, offensive, or threatening language is strictly prohibited on any platform and will be dealt with according to the school's Code of Conduct.
- No staff is permitted to send any posts or information that could damage the reputation of school or cause any disruption to the smooth running of the school.
- No staff may participate in any personal, prejudicial, or discriminatory attacks against others.
- Staff must not harass others in school or while accessing MS Team platforms from home. Furthermore, they must not use their personal social media platforms to harass any member of the school community.
- It is a criminal offense in the UAE to knowingly send or post false, defamatory, or malicious information or spread rumors.

- No staff at school is permitted to share any private information about another staff or student without their consent. Breaches of this will be dealt with according to the school's Code of Conduct.
- Staff will be held accountable for their behavior online, even if events occur at school.
- All staff must ensure that they do not breach the confidentiality of any member of the school community. Nor must they make threats to or about another or attempt to deface them in any way using any form of social media platform.
- No staff is permitted to access or post any content that can be considered profane or obscene, encourages others to participate in any illegal activities, or shows any violence or discrimination towards other people.
- If any staff accesses any such content mentioned above by mistake, they must inform the IT department immediately; otherwise, they may be held accountable.
- Staff will not deliberately distribute or download any material in such a manner that causes congestion of networks
- Staff should not deliberately access inappropriate websites to download, store or print files or messages that use inappropriate language or degrade others.

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 school we take plagiarism and copyright seriously, and we regularly remind the students of their responsibility to avoid plagiarizing 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.

Behavioural violations

First level

1. Fail to implement ICT in class rooms.
2. Fail to acquire equivalency certificate in the prescribed time.
3. Lack of organizational skill.
4. Fail to follow campus language.

Second level

1. Inability to use online teaching and learning platform.
2. Fail to explore the resources provided by the school for the development of students
3. Not able to acquire TLS in the prescribed time.
4. Exposing personal problems in the class and blend it with professional time.
5. Not following appropriate dress code.
6. Being irregular in school and class.
7. Fail to follow behavioral guidelines set by the school and MoE.
8. Fail to comprehend rights of children set by national and international agencies.

Third level

1. Fail to contribute in the designing and drafting of curriculum plan.
2. Unable to follow and complete the various objectives and feature of curriculum plan.
3. Unable to complete the portions on time and provide enough support to students.
4. Not demonstrating creative and latest pedagogical skills.
5. Not correcting notebooks, assessments, worksheets, projects, records etc.
6. Fail to undertake responsibility to organise school assembly, co-curricular activities, picnic, sports, annual day etc.
7. Fail to communicate with parents effectively with regard to student's achievement and well-being.
8. Not cooperating with school's daily activity plan.
9. Fail to deliver information to parents and students in online and offline platform.
10. Lack of care while handling school property.
11. Undermining the value of teaching by not comprehending motto, vision and mission of the school.
12. Fail to take responsibility for improving teaching through suitable professional development system.
13. Not respecting privacy of the students.
14. Using phone for talking during the class time.
15. Fail to provide safe learning environment.
16. Fail to maintain fair and harmonious relationship with school authorities, staff, students and parents.
17. Misusing the teaching and learning platform of the school.

Fourth level

1. Showing incompetency to fulfill the academic responsibilities set by the school
2. Lack of expected subject knowledge according to the grade handle.
3. Unable to perform invigilation duty during the exam time.
4. Showing discrimination to the students and fail to treat pupil with dignity and honour.
5. Not following a credible and legitimate process in exam evaluation.
6. Unable to provide proper guidance (discipline, littering etc.) to students in the class room and campus.
7. Using improper language in the class room and campus.
8. Not posing as a role model to the students.
9. Being dishonest to institution, staff, students and parents.
10. Improper relationship or contacts with staff and students.

11. Engaging in corporal punishment which may harm physically and mentally to the students.
12. Make malicious or unfounded criticism against colleagues and institution.
13. Engaging in bullying in cyber platforms and face to face class rooms.
14. Sharing confidential information about students, staff and students.
15. Giving grade, promotion or support by accepting gifts, money and favours.
16. Posting personal opinion about students in social media sites and print media.

Fifth level

1. Engage in inappropriate relation on communication in phone or social media.
2. Using drugs or alcohol in the school
3. Showing or sharing immoral or inappropriate digital or non-digital content.
4. Sexting with staff and students in online media.
5. Posting contents in social media or public platform which are against the values set by UAE.
6. Engaging in criminal/illegal activities.

Sanctions

Sanction for breaches of the school Acceptable Use policies will vary depending upon the severity of the violation and wherein they correspond to existing policies in place already at school

1. **Sanctions For first level, second level and third level violations:**
   - The head of the institution will endorse a mentor to give counselling and guidelines to rectify and improve.
   - If there is no expected improvement the head of the institution will directly counsel the staff.
   - If the problem exists with same intensity first warning letter will be provided.
   - If there is no expected improvement second warning letter will be provided.
   - If there is no expected improvement third warning letter will be provided. If there is no modification or improvement in performance, behaviour or attitude the final action is expulsion.

2. Sanctions **For fourth level violation**
   - Warning letter will be issued.
   - If there is no expected improvement second warning letter will be provided.
   - If there is no expected improvement third warning letter will be provided.
   - If there is no modification or improvement in performance, behaviour or attitude the final action is expulsion.
3. Sanctions **For fifth level violation**
   - Expulsion

General and Best Practice

- All staff must ensure that they adhere to the school 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 needs 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 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 Leader, and he will decide upon the course of action to be taken in line with the school Code of Conduct.

Adopted: April, 2017 **Reviewed and updated: March, 2022**

Hameed Ali Yahya K M
Principal
Online- Safety Officer

Staff Agreement Form for Acceptable Use Policy

I have read, understand, and will abide by the school 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 : _____