

KNOWLEDGE GATE INTERNATIONAL SCHOOL

ICT Acceptable Use Policy (AUP) Form

STUDENT

I understand and will abide by the provisions and conditions of this agreement. I understand that any violations of the above provisions may result in disciplinary action and the removal of my privileges. I also agree to report any misuse of the system to a staff member. Misuse may come in many forms but may be viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal activities, racism, sexism inappropriate language, any act likely to cause offence or other issues described above.

Student Name: _____

Form: _____

Signature: _____

PARENT or GUARDIAN

Knowledge Gate International School students must also have the signature of a parent or guardian who has read this agreement.

As the parent or Guardian, I have read this agreement and understand that access to electronic information services is designed for educational purposes. I understand that, whilst the Internet service provider operates a filtered service, it is impossible for Knowledge Gate International School to restrict access to all controversial materials and will not hold the school responsible for materials acquired on the network. I also agree to report any misuse of the system to the school.

I hereby give my permission to Knowledge Gate International School to permit my child access to electronic information services and I certify that the information given on this form is correct.

Parent/Guardian Name _____

Signature _____

Date _____

KNOWLEDGE GATE INTERNATIONAL SCHOOL



ICT Acceptable Use Policy for Students

DOCUMENT CONTROL	
Policy Reference	KGIS - ICT Acceptable Use for Students - 011
Date Adopted	August 2019
Last Review Date	August 2024
Next Scheduled Revision (biannually)	February 2025

Version	Author	Date	Changes
V 0.4	Mahesh Maniyeri	19 May 2019	<p>Added section VPN, VPS Services.</p> <p>Added section Laptops /iPads/Tablets/School Devices.</p> <p>Amended the section Use of other technology.</p> <p>Added section mobile phone.</p> <p>Amended the section Disciplinary Procedures</p>
	Andrea Hunt	30 May 2019	<p>Linked to BOYD policy, Use of Mobile Phone Policy.</p>
V 0.5	Mahesh Maniyeri	03 June 2019	<p>Amended the section Laptops / iPads / Tablets / School Devices</p>
V 0.6	Mahesh Maniyeri	25 May 2020	<p>Updated all sections to cover VLE.</p> <p>Added sections: Introduction, The KGIS Network, Cyberbullying, Radicalisation, Education and Awareness & Disciplinary Procedures</p>
V 0.7	Mahesh Maniyeri	15 September 2021	<p>Amended section 2 Responsibilities</p> <p>Amended section 3 Security</p>
V 0.8	Hussein Ali	22 May 2022	<p>Amend Section 1 introduction</p> <p>Amended Section 2 Responsibilities</p> <p>Amended Section 3 Security added links</p> <p>Amended Section 6 Internet</p> <p>Amended section 6.6 social networking sites</p> <p>Amended section 7 Laptops / iPads / Tablets / School Devices</p> <p>Added policy links to section 8 cyberbullying</p> <p>Added policy links to section 13 mobile phones</p> <p>Changed students to students.</p>

V 0.9	Mahesh Maniyeri	06 February 2024	Amended section 1.4 Added section 2.3.19 Added section 7, AI & VR Guidelines
-------	-----------------	------------------	--

Table of Contents

1. Introduction
2. Responsibilities
3. Security
4. The KGIS Network
5. KGIS Email – including Gmail & Outlook
6. Internet
7. Laptops / iPads / Tablets / School Devices
8. Cyberbullying
9. Radicalisation
10. Use of Other Technology
11. VPN & VPS Services
12. Personal Laptops / Computers
13. Mobile Phones
14. Return of the ICT Acceptable Use Policy Form
15. Education and Awareness
16. Disciplinary Procedures

1. Introduction

- 1.1. The purpose of the ICT Acceptable Use Policy is to ensure that students at the KGIS are able to take advantage of the potential of ICT to support and enhance their learning in a responsible and secure manner.
- 1.2. This policy applies to all relevant digital devices, i.e. not just desktops and laptops, but also smartphones, tablets and wearable devices are applicable. The policy applies to both School and privately-owned equipment brought on site by either students, staff or third parties, as well as School and privately owned equipment used to access KGIS services and data.
- 1.3. Knowledge Gate International School believes in the educational benefits that can be offered to students through the correct and appropriate use of technology. However, it is acknowledged there is a need to address the dangers and raise awareness of potential abuses of technology. Good planning and management at KGIS will ensure appropriate and effective staff and student use.
- 1.4. This policy is designed primarily to safeguard students, but also to provide guidance for adults in positions of responsibility. It applies to all members of the KGIS community, including students, teachers, support staff, visitors, volunteers and temporary staff. It is not limited to the school network; it is designed to cover all aspects of Online Safety that may impact on the school community. The policy also includes the usage of all forms of ICT, including but not limited to computers, laptops, tablets, smartphones, virtual reality (VR) equipment, and software applications provided by the school.
- 1.5. The safe and appropriate use of technology is not a standalone issue. This policy should be read in conjunction with a number of related policies.
- 1.6. To ensure this outcome, our students and their parents need to understand the rules and systems that we have put in place to protect our users and school system.

2. Responsibilities

- 2.1. The KGIS SLT will ensure both the Acceptable Use of IT Policies and related policies are implemented. These policies will be reviewed during the course of each academic year or post any specific technological developments by The IT Department, prior to being endorsed by the Executive Headmaster.
- 2.2. All users of digital technology at the KGIS are expected to act responsibly and to show consideration to others.
- 2.3. It is not acceptable to:
 - 2.3.1 Download or install any programs or games to a school-owned computer.
 - 2.3.2 Introduce a virus or malicious code.
 - 2.3.3 Bypass network and systems' security.
 - 2.3.4 Access or use another person's account.
 - 2.3.5 Trying to gain access to an unauthorised area or system.
 - 2.3.6 Use any form of hacking or cracking software.

- 2.3.7 Connect or install any networking device (router, switch, wireless access point, etc.) to the network or via a computer.
- 2.3.8 Connection to the internet using a 3G or 4G enabled technology is strictly forbidden within school grounds and classrooms.
- 2.3.9 Access, download, create, store or transmit material which is indecent or obscene, or material which could cause annoyance, offence or anxiety to other users, or material which infringes copyright, or material which is unlawful.
- 2.3.10 Engage in activities that waste the technical support time and resources of the KGIS.
- 2.3.11 Take food or drink of any kind into the ICT rooms.
- 2.3.12 Willfully damage or tamper with any network equipment.
- 2.3.13 Share any materials with students or staff outside of KGIS.
- 2.3.14 Video online learning lessons, meetings or events.
- 2.3.15 Photograph online learning lessons, meetings or events.
- 2.3.16 Browse, download, upload or forward material that could be considered offensive or illegal
- 2.3.17 Share online meeting codes (Zoom, MS Teams, Google Meets etc) with anyone else.
- 2.3.18 Use VPN services to access blocked sites and online services, such as online gaming and streaming services.
- 2.3.19 Any unauthorised or inappropriate use of ICT tools, including AI and VR technologies, is strictly prohibited.

3. Security

- 3.1 Each student is responsible for keeping their login secure and should not share it with anyone else.
- 3.2 No student is allowed to use a computer allocated to a member of staff.
- 3.3 No user should log on as someone else, nor use a computer which has been logged on by someone else.
- 3.4 Users who are going to be away from their workstation for 10 minutes or more should log off their account.
- 3.5 Access to the Internet is filtered to prevent access to inappropriate sites and to protect the computer systems. Users should be aware that the school logs the internet use of all users.
- 3.6 Users should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- 3.7 It is illegal for students to take and store photographs of staff or students without their written permission (GDPR, [PDPL](#)).
- 3.8 Users should be aware that the school has a right to access personal folders on the network and individual email accounts. Privacy will be respected unless there is a reason to suspect that the ICT Acceptable Use Policy or school guidelines are not being followed.

4. The KGIS Network

- 4.1. KGIS is responsible for ensuring the School Network is as safe and secure as possible, and undertakes to filter content, denying access to material that might prove offensive, inappropriate, promote radicalisation, be illegal or harmful.

- 4.2. These filters are reviewed regularly, but the School cannot guarantee that such material is always inaccessible. All parties should be aware that both staff and students are readily able to access the Internet via either a 3G or 4G unfiltered service, provided by a mobile phone provider, and propagate that access by creating a hotspot. Such activity is deemed highly inappropriate. The School cannot accept liability for any material accessed, or any consequences of internet access.
- 4.3. Students are given training on how to keep safe online, and what to do should they find inappropriate material. They are expected to adhere to the Acceptable Use Policy.
- 4.4. All users are provided with a username and password and will have clearly defined access rights to the school IT systems. The School will monitor the use of communications and online behaviour for all users of the system in order to best ensure that the online environment remains both safe and secure.
- 4.5. It is the responsibility of all staff to adhere to the Safeguarding policies, and these apply just as much to the use of IT systems, either those in the School Network, or outside of it. The three principles of Prevention, Protection and Support should determine any action taken by a member of staff.

5. KGIS Email – including Gmail & Outlook

5.1 All KGIS staff and students from will be provided with KGIS email accounts

5.2 students will be taught how to use email as a communication tool.

5.3 students and staff will be encouraged to ensure that communications with persons and organisations ensures appropriate educational use and that the good name of the school is maintained

5.4 Emails are monitored and filtered. In-coming and out-going email will be regarded as public, in so far as Staff and students are reminded they are provided with email accounts for school use. They should be prepared for any email they send or receive to be intercepted and read by an authorised employee of the school, or any such external agency as appointed by the school, including but not limited to law enforcement agencies.

5.5 Email messages on school business to parents which contain sensitive and substantive information must be approved before being sent by the Executive Headmaster.

5.6 students with individual email accounts, will be held accountable for the use of that account.

5.7 The use of third party email accounts by students at school will be discouraged and where possible blocked. Excessive social email use can interfere with learning and will be restricted.

5.8 For safeguarding purposes, staff are advised only to communicate with students electronically via the student's and member of staff's School email account, unless there are extenuating circumstances and a senior member of staff has been made aware.

5.9 Never open an email attachment sent by someone you do not know or that you are concerned about.

5.10 If this does occur, shut down the computer and inform the IT department immediately.

5.11 Never reveal personal details about yourself, such as your address or telephone number, or arrange to meet someone you do not know in an email.

5.12 Messages must be phrased using appropriate language and a polite tone.

5.13 The forwarding of chain letters is not allowed.

5.14 Staff must tell their manager or a member of the respective SLT if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves. Staff are also required to equate themselves with the School email etiquette document.

5.15 Students should inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

6. Internet

6.1. The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

6.2. Access to the Internet is a necessary tool for staff and is of benefit for the students who show a responsible and mature approach. It should be noted that the use of the computer system at KGIS by both staff and students without permission, or for a purpose not agreed by the school could constitute a criminal offence. Students should be made aware of this by their form teacher/tutor, staff should be made aware of this by the relevant Headteacher.

6.3. Internet use is a part of the KGIS curriculum and a necessary tool for staff and students. Internet access is an entitlement for students who show a responsible and mature approach to its use.

6.4. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

6.5. Access to the Internet via a Third Party Carrier whilst on KGIS premises:

6.5.1 With the advancement of technology, access to the Internet via 3rd Party telecommunication systems is now both readily available, affordable and commonplace, for both students and staff.

6.5.2 The School is not able to police such access via 'dongles' or 'smartphones' which allow access via mobile broadband but it is aware that students and staff may be able to access inappropriate material via such means.

6.5.3 Therefore, to protect all parties concerned, the school reserves the right to examine any IP enabled device brought into school which has or could be connected to the School network. Approved anti-virus software must where applicable be installed on such devices.

6.6. Social Networking Sites:

6.6.1 The use of such sites (Facebook, Twitter, Pinterest, Instagram to name but a few) has and will continue to increase.

6.6.2 KGIS advises all staff and students to use such a system in an informed manner. Any reference direct or indirect to either the School, or a member of staff, or a student at KGIS must be carefully considered.

6.6.3 The school reserves the right to ask for any comments/postings to be altered or removed that it considers inappropriate which make reference to any member of the school, or the School itself either directly or indirectly.

6.6.4 students are educated on the dangers of social networking sites and how to use them in safe and productive ways.

6.6.5 students are advised never to give out personal details of any kind which may identify them or their location. Instates students are encouraged to use nicknames and avatars when using social networking sites.

6.6.6 They are all made fully aware of the School's code of conduct regarding the use of IT and technologies and behaviour online.

6.6.7 Access to social networking sites as a general rule is prohibited for students, although exceptions may be made where a suitable educational benefit can be cited by a student/member of staff to the Head of IT.

6.6.8 Staff are not permitted to communicate with parents, students or third parties in relation to any issue concerning KGIS on any social networking site or related facilities. For example, direct communication via Facebook and Twitter is prohibited. The exception being via school or departmental accounts authorised for use by the Executive Headmaster, in adherence with the published guidelines.

6.6.9 students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory.

6.6.10 The School expects all staff and students to remember that they are representing the School at all times and must act appropriately.

6.7. Appropriate & safe access to the internet

6.7.1 In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students.

6.7.2 The school will supervise students and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked

nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a terminal.

6.7.3 The School cannot accept liability for the material accessed, or any consequences thereof.

6.7.4 While no technological solution can be 100 percent effective in guaranteeing safety when using the internet and related technologies, technology can help to minimise the risks to students, particularly when supported by a clear acceptable use policy and appropriate internet safety education.

6.7.5 Methods to quantify and minimise the risk will be reviewed annually by KGIS SLT.

6.7.6 Examples of e-safety issues KGIS needs to be aware of, and protect its users from include;

- Content
 - Exposure to age-inappropriate material
 - Exposure to inaccurate or misleading information
 - Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
 - Exposure to illegal material, such images of child abuse
- Contact
 - Grooming using communication technologies, leading to sexual assault and/or child prostitution
- Commerce
 - Exposure of minors to inappropriate commercial advertising
 - Exposure to online gambling services
 - Commercial and financial scams
- Culture
 - Bullying via websites, social media, instant messaging or other forms of communication device
 - Downloading of copyrighted materials e.g. music and films

6.8 students in school are unlikely to see inappropriate content in books due to selection by publisher and teacher.

6.9 Staff will need to ensure that access is appropriate to the user. Primary students will require protected access to the Internet. The oldest secondary students, as part of a supervised project, might need to access adult materials, for instance a set novel that includes references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying or harassment.

6.10 Filtering will be adjusted as appropriate for the audience. For example, a higher level of filtering will be enforced upon Students than will be the case for Staff.

6.11 Staff will check that the sites selected for student use are appropriate to the age and maturity of students.

6.12 students will not at any time be permitted to buy anything over the Internet.

6.13 Staff who become aware that students are able to access any inappropriate material will be required to report the matter, in a timely fashion to the IT Department.

7. Laptops / iPads / Tablets / School Devices

- 7.1. These devices are workplace devices and are to be used in an appropriate manner. Accessing harmful websites or social networking sites for any non-curricular purpose is not permitted.
 - 7.1.1. They can be removed from a student if conditions of use are breached.
 - 7.1.2. They are only to be used for activities directly related to the Learning Area curriculum and used only when directed by the classroom teacher.
 - 7.1.3. They are not to be used to record, distribute, display or upload images or videos of staff, students, or parents on school premises unless this is part of an activity supervised by any other staff member. Any breach of this rule will result in disciplinary action.
 - 7.1.4. They are not to be used to record, distribute, display or upload INAPPROPRIATE images or videos of staff, students or parents at any time.
 - 7.1.5. If a loaned device is damaged or lost, the parent/ student / Staff will be responsible for the cost of repair or replacement of the device. However, in the event of an incident where damage is caused, the school will conduct a full investigation to ascertain responsibility and inform the concerned person/s. In the case of wilful damage or negligence, students will be expected to contribute part or all of the costs of repair/replacement.
 - 7.1.6. School-owned devices should NEVER be taken to an outside computer service for any type of repairs or maintenance. Students should never leave their loaned devices unattended.

8. Cyberbullying

- 8.1. KGIS has a zero-tolerance policy towards bullying, of all kinds. Cyberbullying, as with any other form of bullying, is taken very seriously.
- 8.2. Information about specific strategies to prevent and tackle bullying are set out in the School's [Anti-bullying policy](#).
- 8.3. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person.
- 8.4. It is made very clear to members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.
- 8.5. If an allegation of bullying does come up, the School will take it seriously.

- 8.6. The school will act as quickly as possible to establish the facts. It may be necessary to examine School systems and logs, KGIS or indeed student owned devices to determine the facts.
- 8.7. The incident will be recorded, and when appropriate be referred to third parties, for example the Police Service if deemed appropriate by the Executive Headmaster.
- 8.8. The school will provide support and reassurance to the victim, and if appropriate their family.
- 8.9. /It will be made very clear to the 'bully' that this behaviour will not be tolerated.
- 8.10. If there is a group of people involved, they will be spoken to individually and as a whole group.
- 8.11. It is important that children who have harmed another, either physically or emotionally, redress their actions and the School will make sure that they understand what they have done and the impact of their actions.
- 8.12. If a sanction is used, it will correlate to the school's behaviour policy, and the 'bully' will be told why it is being used.
- 8.13. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their IT account access suspended to KGIS services.

9. Radicalisation

- 9.1. Radicalisation is the process by which individuals or groups come to adopt extreme views on political, religious and social matters, notably with the result of violent extremism.
- 9.2. The School has a duty to protect children from extremist views, and to equip them with the ability to recognise, question and resist any attempts to radicalise during their formative years.
- 9.3. KGIS educates students how to recognise these attempts as well as promoting critical thinking through the PSHCE curriculum.
- 9.4. It is expected that anyone in the community brings to the School's attention any attempts to promote violent extremism

10. Use of Other Technology

- 10.1. Memory cards, USB Flash drives and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with ICT Acceptable Use Policy. Students using such devices must not be connected to the school network without specific permission from a member of the ICT department.
- 10.2. If any headphones/earphones and electronic devices are brought onto the school grounds they must be turned off and not be visible at any time during classes. Please note that the security of these items is the student's responsibility. The school takes no responsibility for the recovery of these items if they are lost or stolen.

11. VPN & VPS Services

- 11.1. Bypassing our security filters is strictly prohibited and puts your device and the school network at risk. If detected, your personal device will be blocked from the network. You will need to visit the IT Support staff in the IT office to have access restored. Repeated offences could result in suspension.
- 11.1.1. **Students' Usage:** Students are strictly prohibited from using VPN services within the school campus at any time. Additionally, they are not allowed to use 3G or 4G data to access the internet while on school grounds. Students are only allowed to connect to the **KGIS-STUDENT** WiFi network, as filtering policies apply specifically to this connection.
- 11.1.2. **Disciplinary Consequences:** Any student found using a VPN, mobile data, a personal hotspot, or connecting to any network other than KGIS-STUDENT (such as KGIS-Staff) will be reported for disciplinary action. Furthermore, any teacher or staff member found to have shared the KGIS-Staff network password or access with students will also face disciplinary action.
- 11.1.3. **Teachers' Responsibility:** Teachers are advised not to use websites or applications that are restricted within Oman and require a VPN for access. Adhering to this ensures compliance with local regulations and maintains a safe online environment.

12. Personal Laptops / Computers

- 12.1. Personal laptops and computers can be connected to the school internet but only after an AUP has been agreed and returned. In addition, all personal computers may be subject to a technician check before being connected to the network.

13. Mobile Phones

- 13.1. The classroom is a workplace and in school, as in society, mobile phones cannot be accessed in the workplace except when using a work-related application. At no time can a personal device be used for filming during class, school devices must be used for this purpose. Mobile phones are governed by the '[Use of Mobile Policy](#)'.
- 13.1.1. Students should use their mobile phones only before or after school or during recess and lunch breaks. In the Senior School students are governed by the 'BYOD Policy'.
- 13.1.2. Teachers may allow students to use a mobile phone in a classroom setting when using an educationally appropriate application under their direct supervision and instruction.
- 13.1.3. If the phone belongs to another student, the appropriate consequences will apply to both the owner of the phone and the offender.
- 13.1.4. Students should display courtesy, consideration and respect for the rights of others whenever they are using a mobile phone.

- 13.1.5. Mobile phones should not be used in any manner or place that could be disruptive to the normal school routine.
- 13.1.6. Mobile phones are not to be used to record, distribute, display or upload images or videos of students, staff or parents on school premises. Any breach of this rule will result in a suspension and loss of phone privilege for 5 weeks.
- 13.1.7. Mobile phones are not to be used to record, distribute, display or upload INAPPROPRIATE images or videos of students, staff or parents at any time. Any breach of this rule will result in a suspension and loss of phone privilege for 5 weeks.

14. Return of the ICT Acceptable Use Policy Form

- 14.1. If the form agreeing to the terms of the ICT Acceptable Use Policy is not returned to the school, agreed by the student and a parent by the deadline that has been set, then the student will not be permitted to access any computers or other networked electronic devices at the school.

15. Education and Awareness

- 15.1. The School considers itself to have a central role in educating students, parents and staff in issues that may affect them in this area. The School provides a programme that raises awareness of technical and behavioural aspects of safety for students, including topics such as advice on grooming and radicalisation, exposure to material that is not appropriate to their age, the sharing of personal information, their online footprint, cyber bullying, sexting as well as the use of social media and digital communication in general.
- 15.2. This is delivered throughout the curriculum generally, and specifically in PSHCE and Computing and IT periods, as well as assemblies. The programme is designed to deliver information and explore issues at a level appropriate to the age of the student, and certain topics will be revisited at appropriate points in each students' development.
- 15.3. This programme also includes sessions run annually, at all four RGS Schools for parents/guardian's, highlighting both the material that is delivered to our students, but also to assist and educate parents, so they are better informed to support their children use technology appropriately.
- 15.4. This policy will be published both internally on our Intranets, as well as externally on the public KGIS website. Its contents will be broadcast to both students, staff and parents at least annually to raise awareness of the responsibilities of all respective parties.
- 15.5. On joining the School students will be asked to acknowledge their awareness of, and agreement to abide by the related student IT code of conduct, including the use of mobile devices. Similarly, staff will be asked to acknowledge their awareness of, and agreement to abide by both this policy and the Staff Code of Conduct.

Any breach of these rules will result in disciplinary action.

16. Disciplinary Procedures

- 16.1. Students and their parents/guardians are reminded that use of School Technology is a privilege and not a right and that everything done on any School-owned computer, network, or electronic communication device may be monitored by school authorities. Students who misuse the computer facilities and contravene the ICT Acceptable Use Policy will be subject to disciplinary procedures.
- 16.2. Any students found to be involved in recording, distributing or uploading inappropriate images or videos of students, parents or staff at any time will be suspended.