

KNOWLEDGE GATE INTERNATIONAL SCHOOL



ICT Acceptable Use Policy for Staff

DOCUMENT CONTROL	
Policy Reference	KGIS - ICT Acceptable Use for Staff - 053
Date Adopted	March 2023
Last Review Date	February 2024
Next Scheduled Revision (biannually)	February 2026

Version	Author	Date	Changes
0.1	Mahesh Maniyeri	06 Feb 2024	Amended section 1.4 Added section 2.5 Added section 5.23

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. Confidentiality
9. Cyberbullying
10. Radicalisation
11. Use of Other Technology
12. VPN & VPS Services
13. Personal Laptops / Computers
14. Mobile Phones
15. Return of the ICT Acceptable Use Policy Form
16. Disciplinary Procedures

1. Introduction

- 1.1. The purpose of the ICT Acceptable Use Policy is to ensure that all staff at the KGIS are able to take advantage of the potential of ICT to perform their work and enhance their productivity in a responsible and secure manner.
- 1.2. This Policy also applies to all employees of a third party, suppliers, contractors, customers, and visitors who are authorised to access and use the KGIS's systems whether on KGIS premises or not.
- 1.3. It's also intended to define which information is authorised to be accessed and used and which data are and is not permitted to use as well as the application of the security measures to protect the confidentiality, integrity and availability of the information processed.
- 1.4. This policy applies to all relevant digital devices, i.e. not just desktops, laptops, and iPads, but also smartphones, tablets and wearable devices are applicable. 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. 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.
- 1.5. This policy is designed to provide guidance for staff. It applies to all members of the KGIS community, including 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 the school community.
- 1.6. The objectives of this Policy are to:
 - 1.6.1. Provide a safe and secure environment for Users, also considering our customers, colleagues, and assets whilst supporting KGIS strategy.
 - 1.6.2. Explain clearly the responsibilities by setting clear requirements and liabilities for acceptable usage of the KGIS computers, mobile/personally owned devices, systems and data.
 - 1.6.3. Set out clear requirements and responsibilities for acceptable use.
 - 1.6.4. Helping to protect the User's information and KGIS's reputation.
- 1.7. 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.
- 1.8. If there is any doubt about the security or acceptability of a particular activity, Users should seek guidance from their line manager, Teacher or the IT Department immediately.

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.
- 2.4. The IT Department will deal with requests for permission or assistance under any provisions of this policy and may specify certain standards of equipment or procedures to ensure security and compatibility
- 2.5 AI and VR Usage: Staff members utilising AI and VR technology in the classroom are expected to integrate these tools into the curriculum in a pedagogically sound manner, aligning with educational objectives and promoting student engagement and learning outcomes. Staff should also ensure the safety and well-being of students when using VR equipment, providing appropriate supervision and guidance.

3. Security

- 3.1 Each user is responsible for keeping their login secure and should not share it with anyone else.

- 3.2 No user is allowed to use a computer allocated to another user.
- 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 workstations for 10 minutes or more should log off their accounts.
- 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 staff and teachers to take and store photographs of any employee or students without their written permission (GDPR, PDPL).
- 3.8. The KGIS and its staff will always be committed safeguards data privacy as complying with the KGIS GDPR policy General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018
- 3.9. 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.
- 3.10 Passwords must adhere to the following rules:
 - 3.10.1 Minimum of 8 characters in length.
 - 3.10.2 Contain both numeric and alphabetic characters (one must be a capital letter).
 - 3.10.3 The password should be periodically changed (every 3 months, at least)

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 radicalization, 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. 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.

- 4.4. 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.
- 4.5. Users should not delete, destroy, modify or interfere with any part of computer equipment, systems or data (e.g. anti-virus software or firewalls), including programs, information, data, any equipment or network or any software used which could have the effect of harming or exposing to risk.
- 4.6. Users should not download any school intellectual property, students or staff personal information including personal files, bank information, photos, and work files to personal devices, storage or any online/offline storage media.
- 4.7. Users should not attempt to gain access to restricted areas of the network, or to any password-protected information. Requests for amended access rights should be directed to the Line Manager and Head of IT.
- 4.8. Users using laptops or Wi-Fi-enabled equipment must be particularly vigilant about its use outside the office and take any precautions required by the IT Department from time to time against importing viruses or compromising the security of the Systems. Systems contain information which is confidential to the KGIS and/or which is subject to data protection legislation.

5. KGIS Email, Instant messaging and Video conferencing

5.1 All KGIS staff will be provided with a KGIS email account

5.2 E-mail, instant messaging and the intranet is a vital business tool but an informal means of communication and should be used with great care, accuracy and discipline

5.3 All staff who use KGIS email services are expected to do so responsibly and they must comply with all applicable laws as well as this policy.

5.4 Staff will be encouraged to ensure that communications with persons and organisations ensure appropriate educational use and that the good name of the school is maintained

5.5 Emails are monitored and filtered. Incoming and outgoing emails will be regarded as public, in so far as Staff and teachers 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.

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

5.7 The use of third-party email accounts by users 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 Messages must be phrased using appropriate language and a polite tone.

5.12 The forwarding of chain letters is not allowed.

5.13 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.

5.14 Users should take care with the content of e-mail/instant messaging, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Users should assume that email/instant messages may be read by others and not include anything which would offend or embarrass any reader, inspired or themselves if it found its way into the public domain.

5.15 E-mail/instant messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail/instant message cannot be recovered for the purposes of disclosure. All email/instant messages should be treated as potentially retrievable, either from the main server or using specialist software.

5.16 Don't Send or forward emails/instant messages that contain anything which may be considered by anyone to be offensive, abusive, obscene, harassing, derogatory, defamatory or discriminatory, including discrimination against others based on their race, sexual orientation, age, disability or religious or political beliefs.

5.17 All staff should not contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them.

5.18 Staff should also refrain from sending confidential messages via e-mail/instant messaging or the internet, or by other means of external communication which are known not to be secure. Any User that receives any of the above from another User via e-mail should inform their line manager or the HR Department.

Users who receive a wrongly-delivered email should return it to the sender. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or used in any way

5.19 Use of video conferencing is for business purposes only. Users are required to act professionally and respectfully at all times.

5.20 Video conferences are required to be treated like a normal meeting with a customer or any other User.

5.21 No foul language or obscene images should be used. If a User's screen is being shared, such User is required to make sure that no confidential data or private information of other Users or customers as well as Inspired confidential information is displayed.

5.22 Users are required to always use the highest security settings during all video conferences.

5.23 Staff members are reminded that when utilising AI platforms, they should refrain from disclosing confidential details or sensitive information, ensuring the protection of student and organisational data.

6. Internet

6.1. Access to the Internet is a necessary tool for staff. It should be noted that the use of the computer system at KGIS by both staff and teachers without permission, or for a purpose not agreed by the school could constitute a criminal offence.

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

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

6.3.1 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.

6.3.2 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.

6.3.3 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.

6.4. Social Networking Sites:

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

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

6.4.3 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.

6.4.4 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.

6.4.5 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 is via school or departmental accounts authorized for use by the Executive Headmaster, in adherence with the published guidelines.

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

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

6.5. Appropriate & safe access to the internet

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

6.5.2 The school will 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.

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

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

6.5.5 Methods to quantify and minimize the risk will be reviewed annually by KGIS SLT.

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

6.5.6.1 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

6.5.6.2 Contact

- Grooming using communication technologies, leading to sexual assault and/or child prostitution

6.5.6.3 Commerce

- Exposure of minors to inappropriate commercial advertising

- Exposure to online gambling services
- Commercial and financial scams

6.5.6.4 Culture

- Bullying via websites, social media, instant messaging or other forms of communication device
- Downloading of copyrighted materials e.g. music and films

6.6. 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.

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 willful 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. Confidentiality

- 8.1. The KGIS takes confidential information very seriously, and there may be serious consequences for any information breaches.
- 8.2. All staff must not use or exploit confidential information for their purposes or the purposes of any third party. This means you can only use confidential information to support the interests of the KGIS.
- 8.3. Users shall not modify, reproduce, duplicate, copy, re-sell or distribute for any commercial/personal purpose any materials or content on Inspired systems/applications without the prior written consent of Inspired or the copyright owner. In particular, it is up to Users to check the terms and conditions of any license for the use of the software or information and to abide by

them. Software and information provided by Inspired may only be used in the course of your duties as an employee of KGIS.

- 8.4. Users must abide by all of the licensing agreements for software entered into by Inspired with other parties.
- 8.5. Staff can only share or communicate confidential information in the proper performance of their duties or if required by law. In all other circumstances, you are not permitted to share confidential information.
- 8.6. Sending confidential information to personal email addresses or storing it on personal devices is strictly prohibited (except where the use of personal devices for work has been expressly authorised).
- 8.7. Any KGIS member leaving the KGIS must return all property belonging to the Group in a satisfactory condition and all confidential information in their possession or control.
- 8.8. If you have a personal computer, any electronic device or a storage system with information belonging to or relating to the business of the Group, copies of that information must be forwarded to your line manager and permanently deleted from your personal device or storage system before you leave the company.

9. Cyberbullying

- 9.1. KGIS has a zero-tolerance policy towards bullying, of all kinds. Cyberbullying, as with any other form of bullying, is taken very seriously.
- 9.2. Information about specific strategies to prevent and tackle bullying are set out in the School's Anti-bullying policy.
- 9.3. 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.
- 9.4. 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.
- 9.5. If an allegation of bullying does come up, the School will take it seriously.
- 9.6. 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.
- 9.7. 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.
- 9.8. The school will provide support and reassurance to the victim, and if appropriate their family.
- 9.9. It will be made very clear to the 'bully' that this behaviour will not be tolerated.

10. Radicalisation

- 10.1. 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.
- 10.2. 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.

- 10.3. It is expected that anyone in the community brings to the School's attention any attempts to promote violent extremism

11. Use of Other Technology

11.1 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.

11.2 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.

12. VPN & VPS Services

12.1 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.

13. Personal Laptops / Computers

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

14. Mobile Phones

14.1 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. The 'Use of Mobile Policy governs mobile phones'.

14.1.1 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.

14.1.2 users should display courtesy, consideration and respect for the rights of others whenever they are using a mobile phone.

14.1.3 Mobile phones should not be used in any manner or place that could be disruptive to the normal school routine.

14.1.4 Mobile phones are not 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.

14.1.5 Mobile phones are not 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.

15. Return of the ICT Acceptable Use Policy Form

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

16. Disciplinary Procedures

- 16.1. Staff are reminded that the 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 staff found to be involved in recording, distributing or uploading inappropriate images or videos of students, parents or staff at any time will be suspended.

ICT Acceptable Use Policy (AUP) Form

KGIS Staff

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 system misuse to an SLT member or the IT department. 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.

Name: _____

Dept/School: _____

Signature: _____

Date: _____