Foundational Document for

Device and ICT Policy

Version 2024

GLOBAL LEADERSHIP ACADEMY
Jeffreys Bay

INTRODUCTION

This ICT and Device Policy is an integral part of the broader policy framework at Global Leadership Academy (GLA) and should be read alongside the GLA Philosophy of Education, School Values, Vision and Mission, and School Description. This policy outlines practical guidelines and regulations to ensure responsible, secure, and effective use of ICT resources. Any misconduct related to ICT, social media, or device use will be managed per the GLA Student Code of Conduct.

DEFINITIONS

- **ICT (Information and Communication Technology)**: Refers to digital tools and resources used for communication, learning, and teaching purposes.
- **Device**: Includes tablets, laptops, mobile phones, and any other technology that can connect to the internet and be used for educational purposes.
- **Monitoring App**: Software such as *Family Link* that parents can use to manage device activity and promote safe usage.
- **AI (Artificial Intelligence)**: Digital tools and programs that simulate human-like capabilities, such as generating text or completing complex tasks. For the purposes of this policy, AI includes any software used to assist or automate schoolwork.
- **BYOD**: Bring Your Own Device

1. MOBILE PHONES

At Global Leadership Academy, we are committed to fostering an optimal learning environment that prioritizes education, collaboration, and personal development. While we embrace modern technology and require learners to use tablets or laptops for educational purposes, we will implement a strict policy prohibiting the use of mobile phones during school hours, effective from 2025.

RATIONALE

- **Enhanced Learning Environment**: Mobile phones are a significant distraction in the classroom. To ensure that students remain focused and engaged in their lessons, the non-use of phones will minimize interruptions caused by notifications and social media.
- **Reduction of Cyberbullying**: Prohibiting mobile phones during school hours will help reduce opportunities for cyberbullying, promoting a safer and more respectful atmosphere for all students.
- **Encouragement of Face-to-Face Interaction**: By limiting phone usage, students will be encouraged to interact directly with their peers and teachers, fostering better social skills and stronger relationships within the school community.
- **Protection from Inappropriate Content**: Mobile devices can provide access to unsuitable material that is not aligned with our school values. By restricting their use, we aim to protect students from exposure to harmful content.
- **Integrity and Academic Honesty**: The use of mobile phones increases the likelihood of cheating during assessments. Our policy aims to uphold the highest standards of academic integrity.
- **Improved Focus on Health and Well-Being**: Excessive screen time associated with mobile phone usage can lead to various health issues, including anxiety, sleep disturbances, and diminished physical activity. A mobile-free school day promotes healthier habits and well-being.

- **Parental Responsibility**: We encourage parents to engage with their children regarding mobile phone use and support this policy by ensuring that phones are not brought to school. Parents will be held accountable for the content and usage on devices registered in their children's names.

IMPLEMENTATION

- Students are required to leave their mobile phones at home or with a designated area (locker) in the school during school hours.
- Any student found in violation of this policy will face disciplinary action, as outlined in the Global Leadership Academy - Student Code of Conduct.

By implementing this policy, Global Leadership Academy aims to create an environment conducive to learning, growth, and positive interactions among all members of our school community. Your support in reinforcing this policy at home is greatly appreciated.

2. RISK ASSESSMENT & RESPONSIBILITY

Students are expected to demonstrate appropriate and responsible behaviour when using the School's ICT facilities as well as when using their own personal Devices.
Students are expected to comply with the specified guidelines and rules set out below. Necessary disciplinary action will be taken against Students who disregard this policy.
Students bring their Devices to use at their own risk.
Students are personally responsible for keeping their Device up-to-date and secure.

The School is in no way responsible for:
- Maintenance of any Device.
- The loading, charging, back-up, updating of apps etc.
- Broken Devices.
- Lost or stolen Devices.

2.1 SECURITY

In order to use the school's computers, learners' own devices, and school systems, each learner must use their allocated username and password. Learners must not use a password belonging to another person, or attempt to access any files where they have not been authorised. Passwords must remain confidential and learners must not allow others to access the network with their personal password. Learners must not gain or attempt to gain unauthorised access to any computer system(s) for any purpose. Such hacking or attempted hacking is a criminal offence under the Electronic Communication and Transaction Act, Act 25 of 2002. The following is not permitted on school IT equipment without personal permission from the Head of IT Services:

- Changes to installed software or hardware configurations
- Downloading and/or installing software on school equipment

2.2 ANTI-VIRUS

Potential sources of viruses include shared devices such as DVDs, USB Memory sticks, email (including, but not limited to, files attached to messages), and software or documents copied over networks and downloaded from the Internet. In order to protect against the virus threat, anti-virus software is installed and updated regularly on all school PCs. Any pupil-owned PCs, laptops or mobile computing devices connected to the network must have Anti-Virus software installed.
Any device that is found not to have Anti-Virus software, or that does not have a recent update, will be removed from the network until remedied.

2.3 INTERNET ACCESS AND USE OF ICT

Internet safety depends on staff, parents and the learners themselves taking responsibility for the use of Internet and other communication technologies on their devices. The balance between educating learners to take a responsible approach and the use of regulation and technical solutions must be judged carefully.
Technology could present dangers including sex, violence, racism and exploitation from which learners need to be protected. At the same time, they must learn to recognise and avoid these risks – to become "Internet Wise". The ICT Development program needs to ensure that students are fully aware of the risks, perform risk assessments and implement remedial and preventative measures to protect themselves and others against these risks. Learners may obtain Internet access in public access points and in homes – Ideally a similar approach to risk assessment and Internet safety should be taken in all these locations by the learners.

2.3.1 Internet Access

General Use - Learners are granted access to the internet to conduct research, complete assignments, and participate in curriculum-based activities. All internet use must align with school rules and regulations to create a positive learning environment. Personal internet access, via any device (e.g. computer, tablet) must adhere to the policies laid out in this document when doing so on the school grounds.

2.3.2 Illegal Activities

Learners must not, by using any service, possess or transmit illegal material. Learners should be aware that as the internet is a global network, some activities/material which may be legal in SA, may be illegal elsewhere in the world and vice versa. If you are in any doubt as to the legality of anything, don't do it.

2.3.3 Downloading

Downloading certain file types can introduce viruses and other security threats and should only be done from a trusted source.

2.3.4 File Sharing (Peer to peer networking)

Sharing of files and downloading of files over peer to peer network connections is only allowed when downloading educational content, that is not copyrighted.

2.3.5 Offensive Material

The Internet has excellent educational potential for learners, but is also of major concern with its ease of access to seriously offensive sites. If you inadvertently come across a site which contains offensive material, you must report this matter immediately to your teacher or to the Head of IT Services. Anyone found attempting to access, or who is in possession of offensive material, will be reported and the necessary disciplinary steps taken.

It is a criminal offence, even for a child, to create, download, possess, distribute or display any pornography, as well as to show such material to a child even if the person showing such material is a child themselves.

2.3.6 Social Networking Websites

Access to Social Networking Websites are not permitted during school times.

2.3.7 Online Email

Access to online personal email services (such as Hotmail or Google mail) is not permitted during lesson times.

2.3.8 Internet access via a Proxy

Accessing the Internet via a third party ‘proxy’ website is strictly prohibited at all times.

2.3.9 Instant Messaging (IM)

The use of Instant Messenger services is not permitted during school times.

2.3.10 Chat Rooms

The use of Chat Rooms is not permitted during school times.

2.3.11 Streaming Media

Schoolwork-related streaming audio and video media accessed via the miEbooks app is permitted during lesson times.

2.3.12 Plagiarism and the Internet

Plagiarism is the theft of ideas and works from another author and passing them off as one's own. Students should be aware that plagiarism is not only cheating, but when it is copied, it is an illegal infringement of copyright.

Learners will also be severely penalised when handing work in to teachers for assignments and tasks which are plagiarised from the Internet or other sources.

2.3.13 School references

Should learners directly refer to the school on any internet website, all comments must adhere to the school’s behaviour rules that require learners to be responsible, thoughtful and considerate and to bring credit to the individual and the school.

2.3.14 Network Usage

There are Wireless and/or Wired network facilities provided at the school. The facility is provided for study purposes during the normal school day. To request connection, you should contact the Head of IT Services who will provide the relevant instructions.

2.3.15 Games

Licensed and approved games are allowed at specific times and under supervision that excludes lesson times and must only be accessed with permission.

2.3.16 Removable Media

Use of removable storage media (for example USB devices) is permitted only where no additional software installation is required.

2.3.17 Portable Media Players

Portable media players (e.g. iPods and MP3 players) may not be connected to the School computer network.

2.3.18 Digital Storage media

Personal pictures files and images (e.g. JPG or BMP files) must not be stored on the network. Personal audio files (e.g. MP3 or WMA files) must not be stored on the network. Personal movie files (e.g. MPG or WMV files) must not be stored on the network. School work related media files may be stored on the network.

2.3.19 Printing

Printing facilities are provided according to the rules and regulations as spelled out by the Head of IT services, at a cost, which will be conveyed to all learners.

2.3.20 Video Recording

Integrated or attached computer ‘webcams’ may be used for educational purposes only to record video with prior permission from the persons you are recording and the teacher responsible.

2.3.21 Weblogs/Blogging

Learners are permitted to contribute to weblogs, but must ensure that any comments or pictures etc. adhere to the school’s behaviour rules that require you to be responsible, thoughtful and considerate and to bring credit to yourself and the school.

2.3.22 Cyber-bullying

Cyber-bullying is defined as bullying via computer functional devices, static or mobile, by the use of social media sites, email, text messages, instant messaging, personal websites and/or chat rooms. Cyber-bullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones/Tablets.

Any suspected cyber-bullying (whether during school time or otherwise) will immediately be reported.

Cyber bullying could consist of:

- Repeated e-mails or IMs sent
- Following the child around online, into chat rooms, favourite Web sites, etc.
- Building fake profiles, Web sites or posing as child's e-mail or IM
- Planting statements to provoke third-party stalking and harassment
- Signing child up for porn sites and e-mailing lists or junk e-mail and IM.
- Breaking into their accounts online
- Stealing or otherwise accessing their passwords
- Posting images of the child online (taken from any source, including video and photo/Tablet phones)
- Posting real or doctored sexual images of the child online
- Sharing personal information about the child
- Sharing intimate information about the child (sexual, special problems, etc.)
- Sharing contact information about the child coupled with a sexual solicitation ("for a good time call …" or "I am interested in [fill in the blank] sex…")
- Encouraging that others share their top ten "hit lists," or ugly lists, or slut lists online and including the child on that list.
- Posting and encouraging others to post nasty comments on a child's blog.
- Hacking a child's computer/profile and sending a child malicious codes.
- Sending threats to others.
- Copying others on a child's private e-mail and IM communications.
- Posting bad reviews or feedback on a child without cause.
- Registering a child's name and setting up a Web site or profile.
- Posting rude or provocative comments while posing as a child (such as insulting racial minorities at a Web site devoted to that racial minority).
- Sending spam or malware to others while posing as a child.
- Breaking the rules of a Web site or service while posing as a child.
- Setting up a vote for site (like "hot or not?") designed to embarrass or humiliate a child.
- Masquerading as a child for any purpose.
- Posting a child's text-messaging address or cell phone number online to encourage abuse and increase a child's text-messaging or cell phone charges.
- Launching a denial of service attack on a child's Web site
- Sending "jokes" about a child to others or mailing lists.

2.3.22 AI Usage Policy

AI technology has both benefits and risks in educational settings. To maintain academic integrity and encourage original work:

- **Permitted Use**: Learners may use AI tools only as part of formal classroom instruction, under the guidance of their teacher.

- **Restricted Use**: AI tools are not permitted for completing homework, assignments, assessments, or language edits. Using AI in these contexts undermines the educational process and will be subject to disciplinary action, as outlined in the GLA Student Code of Conduct.
- **Ethical Considerations**: Learners should understand that while AI can be useful, its misuse compromises the learning experience. Parents should discuss the importance of ethical AI use with their children.

2.4 DEVICE MANAGEMENT

While the school acknowledges that devices have become an important and useful means of communication, it is also aware of the fact that their use and abuse, particularly by children, pose social, ethical and safety consequences.

2.4.1 Usage regulations

It is the duty of the school to alert learners who have devices in their possession, while they are at school or in school uniform, of the following:

- Learners who carry or use devices in public, particularly when travelling to and from school, may become the targets of criminals who accost them and rob them of their devices and other possessions. These attacks occur most frequently when learners are seen using their devices, particularly if they are expensive and/or “latest models” of sought-after brands.
- Learners must not be careless with their devices and leave them lying around or in blazers and bags which are left unattended. Lost and mislaid devices are frequently claimed to be stolen when this is not the case.
- Devices can be used to cheat in examinations and tests. For this reason, no device is permitted in examination venues or in teaching venues when tests and examinations are written, unless otherwise instructed by the teacher. This same policy applies to the externally set national examinations.
- Devices are increasingly multi-functional, offering an array of features which are designed to attract and entertain users. The ready availability of these features means that learners with devices tend to access and use these features in the classroom, becoming distracted from their work. Learners with low levels of self-discipline, poor concentration and/or a poor work ethic are more likely to become distracted by these features.
- Devices can make learners vulnerable to approaches by undesirable individuals or groups including criminals and paedophiles.
- Devices may carry private and personal material, including photographs, video clips, voice messages and personal details which may become accessible by undesirable individuals and groups when devices are lost, borrowed or stolen.

The school will not take responsibility for the theft or loss of any device, no matter what the circumstances.

Learners who do bring devices to school, are required to ensure that it is:

- Not audible or visible while they are in the school building, except with permission in the class.

- Is not on their person when they are writing any test, unless with the permission of the teacher, and not in the examination venue when they are writing examinations.

2.4.2 Purchasing and Insurance

The school will suggest the minimum requirement of the model of device to be purchased by parents. Parents must purchase the device as suggested or a model with extended capability. It is the responsibility of the parents to research which model is best (taking in account the recommended model) for their child.

We recommend that the device is insured by the parent. The school will take no responsibility in case of breakage, loss or damage of any kind. It is the parent's responsibility to take care of any repairs that need to be done.

2.4.3 Battery Charging

Learners need to charge their devices overnight, so that it is sufficiently charged when they get to school. If used for Educational purposes only, as it should be used during the school day, the battery life should quite easily last for the whole school day. Learners will NOT be afforded the facilities to charge their devices at school, as the school does not have adequate facilities to accommodate this.

A flat battery or device left at home, will be treated in the same as if a book had been left at home.

2.4.4 Tablet etiquette in the classroom

- Act responsibly by only using your tablet for educational purposes in the classroom.
- Take out your tablet/earphones/turn on the sound only when requested by the teacher.
- Show respect to the teacher by maintaining eye contact while he or she is talking.
- At the end of the lesson, respect your belongings by packing the tablet (sound off) and earphones away to ensure safety.
- Respect people's right to privacy by not photographing anyone in the classroom.

2.4.5 Taking Care of Devices

2.4.5.1 General Precautions

- Devices must never be left in an unlocked locker, unlocked car or any unsupervised area.
- The device is the property of the learner & parent.
- Only use a clean, soft cloth to clean the screen - no cleansers of any type.
- Cords and cables must be inserted carefully into the device to prevent damage.
- Do not use an incompatible charger to charge your device.

2.4.5.2 Carrying devices & protective cases

- A protective case must be bought by the parent. An investment in a very good protective case would be wise. The protective case must have sufficient padding to protect the device and provide suitable means for carrying the device within the school.

- The guidelines below should be followed:
  - Devices should always be within the protective case when carried.
  - Some carrying cases can hold other objects (such as folders and workbooks), but these must be kept to a minimum to avoid placing too much pressure and weight on the device screen.

2.4.5.3 Screen care

- The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.
- Do not lean on the top of the device when it is closed.
- Do not place anything near the device that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Clean the screen with a soft, dry doth or anti-static cloth.
- Do not "bump" the device against lockers, walls, car doors, floors, etc. as it will eventually break the screen.

2.4.5.4 Screensavers and background photos

Inappropriate media may not be used as a screensaver or background photo. This includes, but are not limited to images containing the presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, gang related symbols, etc.

2.4.5.5 Inspection

Learners may be selected at random to provide their device for inspection and if deemed educationally necessary, the school may request the parent/guardian to reset the device to factory default settings. This could be related to undesirable content being found on the device, or a lack of space to accommodate the educational needs, due to games, photos, videos etc. of a private nature taking up space on the device.

2.4.5.6 Software upgrades

Upgrade versions of licensed software or apps are available from time to time. All updates must be done by the learners or parents. The device software must be up to date at all times.

ITSI will make available the latest Android operating system, as well as the latest MiEbooks app version as a free download when connected to the school server.

2.5 REGULATION

The use of ICT resources brings with it the possibility of misuse as well the inherent dangers including sex, violence, racism and exploitation. It is therefore the aim of this policy to regulate how learners utilize ICT resources, what content they access, as well as their interaction with other ICT users. As with any other regulation this will be done within the framework of inter-alia the

Constitution of South Africa, the laws that govern our country, the policy of the school, as well as all applicable social and ethical standards. As such, transgressions of the policy must be dealt with in accordance with the prescribed remedial steps.

Misconduct in relation to the usage of ICT could constitute a minor breach of school policy, or it could constitute a socially embarrassing incident, or a criminal act, breach of a person's constitutional rights or even cause an international incident.

Misconduct in relation to ICT could be a breach of the following Acts and could constitute a civil or criminal transgression:

- Infringement of a person's constitutional rights in relation to dignity, respect, right to privacy etc.
- Hate speech or racist comments
- Illegal access to information
- Illegal interception of communication
- Harassment
- Slander
- Defamation of character
- Fraud & Corruption
- Extortion
- Copyright & Plagiarism
- Transgressions in terms of child pornography

In relation to a breach by or against a learner of any of the above transgressions, the school, its employees, parents and learners have a legal obligation to report it to the authorities. The parties involved will be encouraged to report the matter to the South African Police Services.

2.6 REMEDIAL ACTION

2.6.1 Monitoring

The school has the obligation and right to monitor, record and copy any and all utilisation of the ICT infrastructure of the school for the purpose of ensuring that the school rules are being complied with and used for legitimate purpose.

If a learner chooses to bring his/her own ICT device, including devices, to school, the school has the right to monitor, record, copy any and all utilisation of such ICT devices for the purpose of ensuring that the school rules are being complied with, and that it is being used for legitimate purposes.

2.6.2 Remedial Process

Situations will exist where the school will have to take action against a learner for breaching the ITC Policy, or to protect the learner against external transgressors or to protect a learner against another learner. In all these situations the school must act in a correct and decisive manner. It is therefore necessary that the process which must be clearly defined and communicated with all staff, learners and parents and that it must be clear that the school will act in the interest of justice and in the interest of the learner.

If a transgression is reported or suspected, the school, in line with the South African Schools Act, will take the necessary actions by monitoring, recording, copying or taking possession of any ICT device, whether private or property of the school. The said device will be accessed by the school, representative of the school or person appointed by the school to establish the validity of the suspicion or report.

A charge will be compiled based upon the facts established and the necessary action will be taken against the learner.

The school will endeavour to resolve all matters with the utmost care and confidentiality and to resolve all matters in an agreeable manner, if possible, internally. If not, the parties will be referred to the South African Police Services.

If there is a legal obligation on the school to report any action to the authorities, the school will endeavour to do so with the utmost care and confidentiality.
The parent or guardian of any learner involved in any transgression will be contacted and notified prior to any action being taken.

3. SOCIAL MEDIA POLICY & GUIDELINES

3.3.1 Policy
This Policy applies to all sectors of the school – teachers, administrators, Parents and students.

- When teachers are using or allowing the use of social media in schoolwork either in classrooms or as required work outside of classrooms, they should regard participation in such online media as an extension of their classrooms and anything which is permitted in class is acceptable online, and anything which would be unacceptable in a classroom should also be unacceptable online.
- In particular, any bullying, insulting, racial or sexist language, or derogatory or offensive comment is forbidden, as is any practice which is at odds with the school's values and practices.
- Nothing should take place online which might bring the school into disrepute.
- Staff, parents or pupils should not abuse any privileged or confidential information they might have access to in any way in private social networking media.
- Teachers should not befriend on Facebook any of their pupils who are still at school, except in the case of a site specifically set up for professional purposes.
- Where staff, parents or students are engaging in online activities outside of direct classroom or boarding house activities, they must remember that social media are by their very nature public documents, and appropriate care needs to be taken when using them.

- Where staff are identified with the school and are engaged in inappropriate fashion, the school can intervene to prevent reputational damage to the school. Such abuse of the media could result in disciplinary action.
- Where students are identified with the school and are engaging in inappropriate fashion, the school will intervene to prevent damage either to the school or to the individuals involved. When students conduct themselves inappropriately without being identified as connected with the school, parents must accept their roles in managing the private activities of their children. They should not expect the school to police the private and out of school activities of pupils of the school; but the school might choose to intervene in such situations if it is in the best interests of the child to do so.

3.3.2 Guidelines

These guidelines for pupils are provided as support and guidance to ensure that practices do not result in transgressions of policy.

- Be responsible for whatever you write. Be aware of what you post online. Social media venues are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.
- Be cautious about publishing photographs, providing personal details including surname, phone numbers, addresses, birth dates and picture.
- Where there is a possibility that you may be identified or associated with Global Leadership Academy, you should act in a manner which is consistent with the general philosophies and values of the school, and not in a manner which might bring the school into disrepute.
- Follow the school's code of conduct when writing online. It is acceptable to disagree with someone else's opinions, but if you do respond in a respectful way. Make sure that criticism is constructive and not hurtful.
- Do not share your password with anyone else, and change your passwords regularly to protect your privacy.
- Do your own work! Do not use other people's intellectual property without their permission. It is a violation of copyright law to copy and paste other's thoughts. When paraphrasing another's idea(s) be sure to cite your source with the URL. It is good practice to hyperlink to your sources.
- Be aware that pictures may also be protected under copyright laws. Verify you have permission to use the image or establish that it is under Creative Commons attribution.
- How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity, or by creating a fictional persona which can be linked back to you.
- Blog and wiki posts should be well-written. Follow writing conventions including proper grammar, capitalization, and punctuation. If you edit someone else's work be sure it is in the spirit of improving the writing.
- If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell a member of staff right away.

4. ADHERENCE AND CONSENT

By signing the School’s ICT Policy, you agree to all the points mentioned, adhere to the rules of the school and hereby give consent and authority to take the necessary actions, including, monitoring, recording, copying, accessing or taking possession of any ICT device, whether private or property of the school.

Parents and learners must understand and agree to the following key points:

- I am excited to be part of my School’s e-learning programme. I understand that the use of the technology is a privilege, not a right. I will use the device and associated technologies in ways that are appropriate, meet school expectations and are educationally beneficial.
- I will take full responsibility for managing my device – including software updates, charging and general care.
- I will never leave the device unattended and I will know where it is at all times.
- I will be a responsible user of the technology and I will not access inappropriate sites or information.
- I will only have recommended apps on my device during school time as to not be distracted by games, social media, etc.
- I will keep food and beverages away from the device since they may cause damage.
- I will protect the device by only carrying it while in the case provided.
- I understand that the device is subject to inspection, and possible factory reset.
- Internet use must support educational objectives.
- AI tools may only be used under direct instructional guidance.
- Parents must monitor and oversee device usage regularly.
- Devices must be charged before school to prevent interruptions.
- **Mobile phones are not allowed during school hours, including breaks and between periods.**
- Cyberbullying and misuse of digital communication are not tolerated.
- Parents are legally accountable for the content on their child’s registered devices.

Date: _______________

Student Name: ______________________

Student Signature: _______________________

Parent/ Guardian Name: ______________________

Parent/ Guardian signature: _______________________