: Learners Today.. Leaders Tomorrow :

The Gulf English School

'Bring Your Own Device' Policy (BYOD)

Date: October 2026
Author: E-Learning Manager/LT

Adoption / Review	Committee	Lead Personnel	Review Date:
October 2026	ELT, LT	E-Learning Manager	October 2027

This policy applies across all campuses:
GES Gharafa (Infants, Juniors, and Secondary) GES Bin Omran

The Gulf English School's

Responsible, Respectful, Resilient

Our Vision

We aim to develop a responsible, respectful, resilient school community, supporting the highest level of personal achievement in a changing modern intercultural world.

V1	We aim to develop a responsible, respectful, resilient school community,
V2	supporting the highest level of personal achievement
V3	in a changing modern intercultural world.

Mission Statements

M1	We provide a high-quality education, focusing on skills, knowledge and application, enabling our community to strive and achieve excellence
M2	We aim to develop a culture of life-long learning, independence, ambition, which is continuously demonstrated by our community.
M3	Our community promotes diversity and global citizenship where individual differences are understood and celebrated.
M4	To drive the development of creative skills and critical awareness in our students.
M5	Our school community provides a safe, supportive, and stimulating learning environment that focusses on the well-being of all
M6	We aim to integrate the use of technology on a day-to-day basis to enhance our teaching and learning.

Our Core Values: The 3 R's

1. **Responsible:** Driven, Ambitious, Achiever
2. **Respectful:** Empathy, supportive, caring, diversity
3. **Resilient:** Risk takers, empowered, committed

Contents

No.	Section
1	What is Bring Your Own Device (BYOD)
2	Rationale
3	BYOD Guidelines
4	Digital Citizenship and Use of AI Tools
5	Mobile Phone Policy
6	User Agreement
7	Reimbursement
8	FAQs
9	Student Computer Use Agreement and Declaration
10	School Liability Statement
11	Shared Agreement of Responsibilities
12	Minimum Recommended Specifications for Laptop / Notebook Computer
13	Examples of Suitable Laptops / Notebooks (For Guidance Only, Not Recommendations)
14	One-Page Summary
14.1	Primary
14.2	Secondary (Years 7–13)

Rationale

The Gulf English School (GES) recognises the important role technology plays in enhancing teaching, learning and communication. Through the appropriate use of digital devices, the school aims to promote personalised learning, collaboration, creativity and independent thinking while preparing pupils with the digital skills needed for an increasingly connected world.

What is Bring Your Own Device (BOYD)

Bring your own device (BYOD) refers to a technology policy where students bring a personally owned device to school for the purpose of learning.

The Bring Your Own Device (BYOD) initiative supports the school's commitment to providing a modern, inclusive and engaging learning environment. It enables pupils to access educational resources, develop digital literacy and extend their learning beyond the classroom.

GES is equally committed to ensuring that technology is used safely, responsibly and effectively. The school promotes positive digital citizenship, online safety and appropriate use of technology in accordance with its three core values: **Responsible, Respectful and Resilient**.

Bring Your Own Device (BYOD)

The BYOD initiative allows pupils to bring personally owned digital devices to school for educational purposes, subject to the school's guidelines and the approval of teaching staff.

For the purposes of this policy, a BYOD device refers to a laptop, notebook, tablet or similar device suitable for supporting teaching and learning. Mobile phones are not classified as BYOD learning devices and are governed separately by the Mobile Phone Policy and GES Online Safety Policy.

Pupils may use approved devices to access educational resources, complete learning activities and collaborate with others when authorised by their teacher. All devices must connect exclusively to the designated GES student wireless network, using individual login credentials. Connections through personal hotspots, mobile data, VPNs or unauthorised wired connections are prohibited unless specifically approved by the IT Network Manager.

The use of personal devices must comply with the school's digital citizenship expectations and relevant policies, including:

- Student Computer Use Agreement and Declaration
- Acceptable Use Policy
- Online Safety Policy
- Whole-School Behaviour Policy
- Safeguarding and Child Protection Policy

Pupils and parents are expected to read, understand and acknowledge the BYOD Policy and associated user agreements. Any misuse of technology or breach of these expectations will be addressed in accordance with the relevant GES policies and campus-specific behaviour procedures. Serious online safety or safeguarding concerns will be referred promptly to the campus Designated Safeguarding Lead (DSL).

GES will continue to review its use of educational technology, online safety arrangements and digital learning practices to ensure they remain appropriate, effective and responsive to pupils' needs.

BOYD Guidelines

- Students may use a privately owned electronic “Internet ready” device on the school’s wireless network with teacher or administrator permission.
- The use of a privately owned electronic device to support and enhance activities is at the subject teacher’s discretion.
- The school wireless network is a monitored service accessed by unique username and password. Inappropriate sites are filtered and blocked when necessary to ensure student use of the internet is for educational purposes.
- Students are prohibited from accessing the Internet using any external Internet service e.g. personal Wi-Fi devices, mobile hotspots, tethering to a phone, mobile data or a VPN. A BYOD device is only to be connected via Wi-Fi access only using the student’s unique username and password. No student shall establish a wireless ad-hoc or peer-to-peer network using his/her electronic device or any other wireless device while on school grounds.
- Voice, video, and image capture applications may only be used with teacher permission and relevant to the learning environment whilst being respectful of the rights of others. Students must never photograph, film or record other students or staff without their permission, and must never share such material online.

- The privately owned electronic device owner is the only person allowed to use the device and their unique username and password associated with the device. In the event that a student believes that his/her password has been compromised, he/she should immediately see IT staff to have the password changed.
- No school software can be installed on personal devices due to the terms of the licenses unless stated otherwise.
- No student shall use any computer or device to illegally collect any electronic data or disrupt networking services.
- Devices are brought to school at the students' and parents' own risk. In the event that a privately owned device is lost, stolen or damaged, the school is not responsible for any financial or data loss.

Where a concern arises about a personal device, staff must refer it to the Head of School and, if safeguarding is implicated, the campus Designated Safeguarding Lead (DSL). Any non-routine examination of a device or its content requires specific senior authorisation and must follow an approved, lawful GES procedure consistent with applicable Qatar requirements, privacy safeguards and the Online Safety Policy. Staff must not routinely inspect private messages or images, and must not view, copy or forward suspected intimate imagery. The DSL will determine protective action and any external referral. Any behaviour consequence will be considered individually under the relevant campus Behaviour Policy, taking account of safeguarding and inclusion needs.

Breaches of this policy will be assessed individually under the relevant campus Behaviour Policy. Responses may include education, parental contact, restricted device or network privileges, restorative or pastoral support and, where justified, proportionate sanctions. Serious online harm must also be referred to the DSL. The school will consider SEND, EAL, medical and safeguarding circumstances before significant sanctions.

Digital Citizenship and Use of AI Tools

All students are expected to be good digital citizens: responsible, respectful and resilient online, in line with our core values (the 3 R's). This applies on every personal device, whether or not it is connected to the school network.

Only age-appropriate, teacher-authorised uses of AI tools are permitted for school learning. Pending adoption of a dedicated GES AI Policy, the following safeguarding, privacy and academic-integrity requirements apply to students and staff using AI tools on personal or school devices:

- Follow your teacher's instructions on when and how AI may be used for a task. If you are not sure, ask.
- Do not present AI-generated work as your own where this is not permitted. Do not use AI in exams or formal assessments unless it is explicitly allowed.
- Do not enter personal information about yourself or others (names, photographs, school records) into AI tools. Staff must not enter identifiable student data into AI tools the school has not approved.
- Never use AI or any other technology to create, change or share images, audio, video or messages that imitate, embarrass, harass or sexualise another person (for example deepfakes,

voice cloning and "undressing" apps). This is a serious breach of this policy and a safeguarding matter, and may be referred to the Police.
- Check what AI tools tell you. They can be wrong or biased.
- Tell a trusted adult if something an AI tool or chatbot says or shows you worries or upsets you.

Further details are in the Online Safety Policy.

Mobile Phone Policy

Our school policies are built on the fundamental principle that students have a right to learn, and teachers have the right to teach. We also believe in courtesy and respect, and this policy aims to encompass these principles.
Students may bring a mobile phone to school at their own risk but must not use it during the school day except under the stated Sixth Form or individually approved arrangements.

How the rule works

- At the start of the school day, students hand their phone to their form tutor. It is returned at the end of the day.
- A student who arrives late signs in at Reception, collects a late slip and hands their phone in at Reception.
- Sixth Form students may keep their phone on their person. They may use it only in the Boys'/Girls' Majlis area and nowhere else on campus.
- Smartwatches, earbuds and any other device that can send or receive messages, access the internet, take photographs or record are treated in the same way as a mobile phone, unless an exception has been agreed.
- Exceptions (for example medical needs or SEND support) are agreed in advance with the Head of School and recorded.

Communication between students and parents

If a parent needs to contact a student, we recommend this to be done through Reception in the appropriate way and not by calling or messaging the student's mobile phone.
If a student is involved in an incident, we would expect that they would notify the school first to enable us to deal with the situation rather than contact the parent first. This would include situations involving illness, conflict with other students or other behaviour management issues.

Consequences for not following this policy:

- Warning to students
- Refer to your year group coordinator
- After school detention
- Confiscation of the phone, with parents/carers informed

Repeated breaches will prompt an individual review by the relevant campus leader, taking account of the pupil's age, circumstances, any SEND or medical needs, safeguarding concerns and previous support. Sanctions will follow the campus Behaviour Policy and will not be automatic.
All students should use their lockers to store valuables.

Staff use of personal devices

- Staff model the expected behaviour. Personal phones are kept out of sight and on silent when teaching or supervising students, and used in staff areas, except for emergencies or approved school purposes (for example multi-factor authentication).
- Staff never use personal phones, personal email, WhatsApp or social media accounts to contact students or parents. Only the school's authorised systems are used.
- Staff do not take photographs or videos of students on personal devices. School-owned devices or approved school accounts are used, and images are kept only on school systems.
- Staff who access school email, Teams or other school data on a personal device must protect it with a passcode or biometric lock, keep it updated, and report loss or theft to IT immediately.
- Staff must not enter identifiable student data into AI tools that the school has not approved.

Parents, visitors and contractors

Parents, visitors and contractors must not use phones or other devices to photograph or record students on site, and should follow any instructions given on arrival. Parents should not message or call their child during the school day and should contact Reception instead.

Safeguarding

Any concern about how a phone or other device has been used, including cyberbullying, sharing of nude or semi-nude images (including AI-generated images) or contact from strangers, is reported straight away to the Designated Safeguarding Lead and handled under the Safeguarding and Child Protection Policy and the Online Safety Policy. Staff must not view, copy or forward such images.

Safeguarding, Child-on-Child Harm and Reporting

Any suspected online grooming, coercion, cyberbullying, discriminatory abuse, sexual harassment, image-based harm, AI-generated intimate imagery, threats or exploitation must be referred without delay to the campus DSL using the authorised GES safeguarding route. The DSL will assess immediate safety, support for affected pupils, confidential recording, parent communication and whether a referral to the appropriate Qatar authority is required. Staff must not investigate suspected intimate imagery by searching, viewing, downloading, copying or forwarding it. A behaviour sanction or restorative meeting must not replace a safeguarding response.

Individual Needs, Accessibility and Equity

Before restricting a device or imposing a significant consequence, staff will consider the pupil's age and developmental stage, SEND, EAL, disability, communication needs, medical monitoring, accessibility and safeguarding circumstances. The Head of School may approve and document individual exceptions, including medical or assistive-technology needs, following consultation with the Inclusion/Learning Support Team, parents and DSL as appropriate. Where a family cannot provide a suitable device, the school will consider reasonable alternative access to learning without disadvantaging the pupil.

Authorisation, Confiscation, Storage and Return

Routine phone hand-in at the beginning of the day is not an intrusive search. Where a prohibited item is surrendered or confiscated, staff will record the reason, pupil, date and time, person receiving it, secure storage location, parent contact where required and the person/date of return. Significant confiscations will normally be reported to parents. Any proposed non-routine examination of belongings or device content must be authorised by the Head of School or a specifically delegated senior leader and handled under an approved Qatar-compliant procedure, with DSL involvement wherever safeguarding is

implicated. Staff must not conduct physical or intrusive searches or inspect private device content without the required authorisation and safeguards. Items will be returned according to campus arrangements unless a documented lawful or safeguarding reason requires otherwise.

Filtering, Monitoring, Privacy and Cybersecurity

Student BYOD devices must use the authorised student Wi-Fi; hotspots, tethering, VPNs and attempts to bypass filtering or monitoring are prohibited unless specifically approved for a legitimate purpose. The IT Network Manager will oversee technical access controls, incident escalation and security, while the DSL retains responsibility for safeguarding decisions. School-network activity may be logged and reviewed by authorised staff for legitimate educational, security and safeguarding purposes in accordance with applicable privacy requirements. This does not give unrestricted access to a pupil's private device content. Users must protect passwords, enable device security updates and report lost devices, suspected account compromise, phishing or inappropriate content promptly.

Incident Records, Parent Communication and Review

Significant BYOD and mobile-phone incidents will be recorded in the authorised campus system, including a factual account, actions taken, authorisation, any device held, parent communication, individual circumstances considered and follow-up arrangements. Safeguarding records will be maintained separately and confidentially through the approved safeguarding route. The Heads of School and E-Learning/IT leads will review implementation and emerging digital risks at least termly, escalating significant safeguarding trends to the Whole-School Leadership Team and reporting key findings to the General Manager and Board as appropriate. The policy will be reviewed annually or sooner following significant incidents, changes to MOEHE requirements or emerging online risks.

Pupil Voice, Parent Concerns and Digital Education

Pupils may report online concerns to a teacher, tutor, trusted adult or DSL without fear of retaliation. The school will provide age-appropriate digital citizenship education and guidance for parents, including safe AI use, online relationships, privacy, cyberbullying and reporting harmful content. Parents may raise concerns through the GES Complaints Policy; urgent safeguarding concerns must be acted upon immediately and not delayed by the complaints process.

Student BYOD and Acceptable Use Agreement

The Gulf English School (GES) is committed to providing a safe, respectful and responsible digital learning environment. All pupils are expected to use school ICT facilities, personal devices, networks and online resources appropriately, in accordance with the school's three core values: Responsible, Respectful and Resilient.
Access to computers and the Internet is provided for the purposes of educational research and learning. Students and parents are asked to carefully read and then sign the following agreement.

By signing this agreement, I confirm that I have read, understood and agree to follow the expectations outlined below.

No.	Student Agreement
1	Educational Use: I will use computers, personal devices, school networks and internet access for authorised educational purposes and follow my teachers' instructions. I will not use games, chat rooms or other non-educational services during learning time unless approved by a teacher.
2	School Network Access: I will connect only to the authorised GES student Wi-Fi network while at school. I

	will not use personal hotspots, mobile data, VPNs or other unauthorised connections to access the internet or bypass school restrictions.
3	Network Security and Monitoring: I will not attempt to bypass the school's internet filtering, security or monitoring systems, access hacking or anonymising services, or disable any approved device-management or security controls.
4	Account and Password Security: I will keep my login credentials confidential, use only my authorised accounts and report any suspected security breaches to a member of staff or the IT Department.
5	Appropriate Online Content: I will not deliberately access, download, store or share inappropriate, offensive, harmful or prohibited content, including material that may compromise the safety or wellbeing of others.
6	Respectful Communication and Cyberbullying: I will communicate respectfully online and will not use technology to bully, threaten, harass, discriminate against, impersonate or humiliate others. I understand that online incidents occurring outside school hours may also be addressed by GES where they affect pupils' safety, wellbeing or school life. Serious concerns may be referred to relevant external authorities where appropriate.
7	Copyright and Intellectual Property: I will respect copyright and intellectual property rights and will not unlawfully download, copy, distribute or share protected software, games, music, images, videos or other materials.
8	Academic Integrity: I will submit my own work; acknowledge information obtained from other sources and clearly identify quotations or permitted AI-generated assistance. I will not present another person's or an AI tool's work as my own where this is not permitted.
9	Privacy and Personal Information: I will protect my own personal information and that of others. I will not disclose or share names, addresses, telephone numbers, financial details, passwords, photographs or confidential information without appropriate authorisation.
10	Responsible Use of Artificial Intelligence: I will follow school instructions when using AI tools. I will not use AI or other technology to create, alter or share misleading, harmful, discriminatory, harassing or sexualised images, audio, videos or messages, including deep fakes or impersonations of others.
11	Photography, Video and Audio Recording: I will not photograph, film or record pupils, staff or other members of the school community without appropriate permission and school authorisation. I will not share recordings or images without permission.
12	Mobile Phones and Connected Devices: I will follow the school's mobile phone procedures, including handing in my phone to my form tutor at the beginning of the school day or to Reception if I arrive late. I will not use mobile phones, smartwatches or other connected devices during the school day unless an approved exception applies. I understand that the specific Sixth Form arrangements remain applicable.
13	School Storage and File Sharing: I will use school digital storage and file-sharing systems only for authorised purposes. I will not store or distribute unapproved games, videos, music, software or other non-educational materials using school systems, or use unauthorised file-sharing applications.
14	Wired Network Access: I will not connect a personal device to the school's wired network without written authorisation from the IT Network Manager. I understand that any breach will be investigated and addressed proportionately under the relevant campus Behaviour Policy, with referral to the Designated Safeguarding Lead (DSL) where safeguarding concerns arise.
15	Reporting Online Safety Concerns: I will promptly inform a trusted member of staff if I encounter harmful content, suspicious messages, cyberbullying, inappropriate contact or online activity that makes me or another person feel unsafe.
16	Compliance with School Policies: I understand that failure to follow this agreement may result in appropriate restrictions on device or network access, proportionate behaviour sanctions or safeguarding intervention, in accordance with the relevant GES Behaviour, Online Safety, Anti-Bullying and Safeguarding and Child Protection policies.

Personal devices are brought to school at the owner’s risk. The school will take reasonable care when a device is formally surrendered or held, and any reported loss, theft or damage will be considered in

accordance with the circumstances and applicable law. This statement does not exclude duties that cannot lawfully be excluded.

Student Declaration and Consent

I confirm that I have read and understood the GES Student BYOD and Acceptable Use Agreement and agree to follow the expectations outlined above.
I understand that access to school ICT facilities, networks and digital resources is provided primarily for educational purposes and that misuse may result in appropriate action in accordance with school policies.

Declaration Details	**To Be Completed by Student**
Student Name:	
Consent / Student Signature:	
Date:	

Parent Agreement:

As a parent/guardian, I confirm that I have read and discussed the Student Computer Use Agreement and the mobile-phone arrangements with my child. I understand that GES applies filtering, monitoring, supervision and safeguarding measures, but that no technical safeguard can eliminate all online risks. I will encourage my child to report concerning content or contact promptly and will use Reception for routine contact during the school day. Nothing in this agreement removes the school's applicable safeguarding responsibilities or legal duties.

Declaration Details	**To Be Completed by Student**
Student Name:	
Consent / Student Signature:	
Parent/Guardian Signature:	
Date:	

Reimbursement

GES will not reimburse students/parents for any of the cost of the device or associated accessories required.

Regulatory Context and Linked GES Policies

This policy complies with applicable Qatar legislation and MOEHE requirements, while drawing on BSO standards, KCSIE 2026, UK DfE guidance and CIS expectations as benchmarks for good practice.
It should be read alongside GES Safeguarding and Child Protection, Online Safety, Anti-Bullying, Whole-School Behaviour, SEND/Inclusion, Data Protection, Acceptable Use and Complaints policies.

School Liability Statement

Personal devices are brought to school at the owner's risk, subject to the school's applicable duties of care and any legal responsibilities that cannot be excluded.

- It is the student's responsibility to ensure that their personal device is kept up to date with the latest operating system updates and upgrades.
- It is the student's responsibility to ensure that their device is kept secure.
- Every student personal device must be protected by password.

A **school** device that a student is using is done so at their own risk.

- It is the student's responsibility to ensure that their given device is kept secure.
- The student / parent is **responsible** if the given device is lost, stolen, damaged or otherwise rendered unusable

In addition, GES **is not responsible** for the following:

- Any **personal** or **school** devices that are broken on school premises or during school visits and outside activities.
- Mobile phones, smartwatches or other devices brought to school, including while they are handed in for safekeeping.
- Any devices that are stolen or lost on school premises or during school visits and outside activities.
- Any personal data that is lost on personal devices while they are being used on school premises.
- Maintaining, repairing and updating devices is the responsibility of the parent / student as the school cannot provide such support.

Shared Agreement of Responsibilities

Responsibility of the student

You agree not to connect to any other wireless or network service that is outside of the school network when using your personal device on school premises, or when taking part in school events and school activities.

By using your own personal device in the school or during school visits and school activities, you agree that you understand the school's Bring Your Own Device policy (BYOD) and that you agree to be bound to the rules, regulations and statements contained in this BYOD policy. This includes the Acceptable Use Policy, Rewards and Sanctions, and the School Liability Statement.

You also understand that the use of a personal device in school or for school activities is for learning purposes only and that it is a privilege, not a right to use your own personal device at school.

You understand that you are fully responsible for the safety, security and care of your personal device when using it in school, during school visits and participation in outside activities."

You also agree to follow the school's mobile phone rules and to use AI tools and all technology honestly, safely and respectfully.

Responsibility of the Parent / Guardian
You understand that GES accepts no responsibility for any loss and/or damage to your children's personal devices that are used in school, during school visits and activities, or when in transit to and from the school.

You should ensure that your child's computer device is fully charged the night before as there are very limited charging points in the classroom.

You understand that by allowing the student to bring their personal device into school, both you and the student agree to these terms and conditions and agree to be bound to the rules, regulations and statements contained in this BYOD policy, including the Acceptable Use Policy, Rewards and Sanctions, and the School Liability Statement.

You agree to support the school's mobile phone rules, to contact your child through Reception during the school day, and to talk with your child about safe, responsible use of technology and AI tools at home.

Responsibility of the school:
We will provide a robust, secure, updated and regularly monitored firewall to filter and block inappropriate sites from the school network as far as is reasonably possible.

Our school network will be swept regularly for virus or malware threats, and appropriate software will be maintained to ensure as far as reasonably possible that the system is free from intrusion.

We will monitor student access to the internet and enforce any measures to ensure that students are not attempting to, or actually, accessing inappropriate or irrelevant sites

We will teach students about online safety and digital citizenship, respond to any concern through our safeguarding procedures, and work with parents to keep students safe online.

FAQs

What is Bring Your Own Device? (BYOD)
Bring Your Own Device (BYOD) refers to technology models where students bring a personally owned device to school for the purpose of learning.

How do I connect to the GES Student wireless network?
Please refer to the following document: Accessing GES Student Wireless Network

Is student internet monitored?
Internet access is filtered whilst they are using the school's network. All Internet activity is logged and monitored accordingly.

Where do I go for support?
If students are not able to connect to the school's wireless network and have followed the steps of Accessing GES Student Wireless Network, they should ask their class teacher to help them connect.

My device was damaged/lost/stolen when I brought it to school. Who should I contact?
Bringing your own device to school can be useful; however, some risks are involved as well. It is always a good idea to record the device's serial number in case of theft and have your own insurance. The school is not responsible for the theft of a device, nor is the school responsible for any damage done to the device while at school. Any time a theft occurs, you should speak with your Learning Coordinator / Head of Year to make them aware of the issue.

Can my child charge their device at school?
It is the responsibility of the student to bring their device to school charged. There are limited charging ports in each classroom so they may not always have access to the ports. **Can my child bring a mobile phone to school?**

Yes, but students may not use it during the school day. It is handed to the form tutor at the start of the day and returned at the end. Late arrivals hand their phone in at Reception. Sixth Form students keep their phone on them and may use it only in the Boys'/Girls' Majlis area. If you need to contact your child, please call Reception.

Can students use AI tools?
AI tools may be used only where age-appropriate and authorised by the teacher. Students must follow academic-integrity, privacy and safeguarding requirements, and must never generate or share harmful, deceptive or intimate content about others. A dedicated GES AI Policy is under development.

Minimum recommended specifications for laptop / notebook computer:

Minimum RAM	4 GB
Minimum Processor	Multi-Core Processor
Minimum Hard Drive	128GB *or higher*
Minimum Screen Size	10" *or higher*
Battery Life	6-8 hours
Operating Platform	Windows 11 / current macOS / current iPadOS
Wi-Fi Connectivity	5 GHz dual-band
Full Keyboard (detachable is fine)	

Examples of suitable laptops / notebooks (for guide only, not recommendation)

Surface Pro
Surface Go
Lenovo 300
Lenovo Think Pad E575
Apple MacBook series
Apple iPad
Chromebook

NB: GES operates on Windows platform.

Primary:

Primary students are ***requested*** to bring their own computer devices into school for use in some lessons.

Secondary Years 7 - 13:

Secondary students are ***requested*** to bring their own computer devices into school for use in some lessons. The recommended minimum specification for this should be as follows:

Minimum System Requirements:

Minimum RAM	4 GB
Minimum Processor	Multi-Core Processor
Minimum Hard Drive	128GB *or higher*
Minimum Screen Size	10" *or higher*
Battery Life	6-8 hours
Operating Platform	Windows 11 / current macOS / current iPadOS
Wi-Fi Connectivity	5 GHz dual-band
Full Keyboard (detachable is fine)	

Examples of suitable computer devices (for guide only, not a recommendation)

Surface Pro
Surface Go
Lenovo 300
Lenovo Think Pad E575
Apple MacBook series
Apple iPad
Chromebook

NB: GES operates on the Windows platform.

Students are not permitted to use their own Wi-Fi or VPN and must access the School Wi-Fi only.