

Bring your own device (BYOD) Policy

Date of policy review:	July 2026
Date for review:	January 2027
Lead for review:	Deputy Head Pastoral & Boarding

Purpose

This policy sets out the conditions under which students may bring and use personally owned digital devices for educational purposes on school premises or during school activities.

Guildhouse school recognises that personal devices can support teaching, learning, organisation, collaboration and independent study. This policy aims to:

- Promote safe, responsible and educational use of technology.
- Safeguard students and staff.
- Protect the school's network and information systems.
- Clarify the responsibilities of students, parents and staff.
- Ensure compliance with safeguarding, data protection and online safety requirements.

This policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- ICT Acceptable Use Policy
- Student Behaviour Policy
- Mobile Phone Policy
- Search, Screening and Confiscation Policy

Definition of BYOD Devices

Permitted devices may include:

- Laptops
- Chromebooks
- Tablets

Mobile phones are not considered educational BYOD devices. Permission to use a personal device remains a privilege and may be withdrawn where expectations are not met.

Student Responsibilities

Students must:

- Bring devices fully charged each day.
- Use devices only when directed by staff or as permitted.
- Access only educationally appropriate content.
- Follow all staff instructions regarding device use.
- Keep devices secure.

- Maintain appropriate antivirus and security updates.
- Report any safeguarding concerns immediately.

Students must not:

- Bypass school filtering or monitoring systems.
- Access inappropriate, offensive or illegal material.
- Photograph, record or livestream others without permission.
- Use devices to bully, harass or intimidate others.
- Interfere with school systems or network security.
- Share accounts or passwords.

Acceptable Use

Personal devices may be used for:

- Classwork
- Homework
- Research activities
- Online learning platforms
- Collaborative learning activities

Personal devices must not be used for:

- Gaming (unless authorised for learning)
- Streaming entertainment
- Social media during lessons
- Gambling
- Unauthorised messaging
- Commercial activities

Network Access

All personal devices connected to the school's network must:

- Use the school's approved wireless network.
- Be subject to and have installed filtering and monitoring software (Securly).

The school reserves the right to:

- Restrict network access.

- Investigate suspected misuse in line with the Search, Screening and Confiscation Policy and Student Behaviour Policy.

Safeguarding and Online Safety

Students must use devices in a manner that:

- Protects themselves and others from harm.
- Supports a respectful and inclusive school environment.
- Complies with the school's safeguarding expectations.

Any use of a device involving:

- Cyberbullying
- Harassment
- Sexting or youth-produced sexual imagery
- Extremist content
- Harmful online challenges
- Unauthorised recording

will be treated as a safeguarding concern and managed in accordance with school policies.

Data Protection and Privacy

Students must not:

- Store confidential school information on personal devices.
- Access staff-only information.
- Share personal information relating to other students.
- Download school records or sensitive information.

Staff will not normally inspect personal devices. However, the school may require a device to be presented where there is:

- A safeguarding concern
- A behaviour investigation
- A network security concern
- A reasonable belief that school rules have been breached

Any action taken will be proportionate and compliant with relevant policies and legal guidance. Any search, screening or confiscation of devices will be carried out in accordance with the school's Search, Screening and Confiscation Policy and relevant Department for Education guidance.

Device Security

Students are responsible for:

- Password protection
- Secure storage
- Charging arrangements
- Software updates
- Antivirus protection

Students should:

- Use strong passwords.
- Enable automatic screen locking.
- Keep operating systems updated.
- Immediately report loss or theft.

Loss, Theft and Damage

Devices are brought to school entirely at the owner's risk.

The school cannot accept responsibility for:

- Loss
- Theft
- Damage
- Hardware failure
- Data loss

Artificial Intelligence (AI)

Where personal devices allow access to AI tools, students must:

- Follow the school's AI policy.
- Use AI only where permitted by staff.
- Acknowledge AI assistance when required.
- Not submit AI-generated work as their own.

Students must not use AI or digital tools to create, alter or distribute misleading images, audio or video of any individual. Misuse of AI may constitute academic misconduct and sanctions in line with the Student Behaviour Policy.

Monitoring

The school reserves the right to:

- Monitor network activity by means of its filtering and monitoring system
- Investigate suspected policy breaches.
- Restrict access where appropriate.

Monitoring will be conducted in accordance with the school's safeguarding and data protection responsibilities and through filtering and monitoring systems to identify safeguarding concerns, inappropriate use, and other behaviour that may place students or the school community at risk. Students and parents are informed that filtering and monitoring systems operate on the school network as part of induction.

Sanctions

Failure to comply with this policy may result in:

- Verbal warning
- Temporary confiscation of the device
- Removal of network access
- Withdrawal of BYOD privileges
- Behaviour sanctions
- Safeguarding referral
- Further disciplinary action where appropriate

Serious incidents may involve parents, external agencies or law enforcement.

Educational Visits

When BYOD devices are permitted on educational visits:

- The same standards apply.
- Staff may place additional restrictions on use.
- Devices must not compromise safety, supervision or safeguarding arrangements.
- The Trip Leader may prohibit or restrict BYOD use during an educational visit where this is necessary to support safeguarding, supervision or educational objectives.

Parent Agreement

Parents/carers acknowledge that:

- Their child is responsible for the device.
- School filtering and monitoring applies.
- BYOD access and use may be withdrawn if expectations are not met.

Monitoring and Review

The school is committed to ensuring that the use of personal devices supports learning, promotes student wellbeing and safeguards all members of the school community.

The effectiveness of this policy will be monitored through:

- Behaviour and safeguarding records relating to device use.
- Trends in incidents involving inappropriate use of technology.
- Feedback from students, staff and parents/carers.
- Reviews of filtering and monitoring reports.
- Emerging guidance, legislation and best practice relating to online safety, artificial intelligence, data protection and safeguarding.

The Deputy Head Pastoral/Designated Safeguarding Lead and Senior Leadership Team will review the implementation of this policy and any significant incidents arising from its use.

This policy will be formally reviewed annually, or sooner where required and any amendments will be approved through the school's policy review procedures and communicated to students, staff and parents as appropriate.

Appendices

Appendix 1: Enrolment/Induction Student Agreement- ICT and Digital Device Acceptable Use Agreement



ICT and Digital Device Acceptable Use Agreement 2026-2027

As a student at Guildhouse School London, I agree to use technology responsibly, safely and respectfully to support learning and contribute to a positive school environment. This agreement applies to all school-owned and personal devices used on school premises, during educational visits, and when accessing school systems remotely.

By signing this agreement, I confirm that I will:

- Use technology responsibly and primarily to support my learning.
- Follow staff instructions regarding the use of devices and technology.
- Treat others respectfully online and not engage in cyberbullying, harassment or inappropriate communication.
- Use only my own accounts and keep my passwords private and secure.
- Respect the privacy of others and not record, photograph or share images, audio or video without permission.
- Report any safeguarding concerns, inappropriate content, misuse of technology or online behaviour that could put someone at risk.
- Use Artificial Intelligence (AI) tools only when permitted by a member of staff and in accordance with school expectations.
- Ensure that any work submitted is genuinely my own and that AI is not used to replace my own learning, thinking or understanding.
- Use only authorised apps, software and online services.
- Take reasonable care of any device I use in school.

I understand that I must not:

- Access, create, store or share inappropriate, offensive, harmful or illegal content.
- Use technology in a way that disrupts learning or negatively impacts others.
- Access another person's accounts, files or information without permission.
- Use VPNs, proxy services, personal hotspots or any other method to bypass the school's filtering, monitoring or security systems.
- Deliberately misuse school networks, devices, systems or digital resources.
- Use AI tools to produce misleading, harmful, offensive, discriminatory or deceptive content, or submit AI-generated work as my own where this is not permitted.

I understand that:

- The school uses filtering and monitoring systems to help keep students safe.
- My use of school technology, devices, networks and accounts may be monitored where appropriate.
- Where there are reasonable grounds relating to safeguarding, behaviour, security or potential breaches of school rules, authorised staff may examine devices, accounts, network records or digital activity in accordance with school policies and legal guidance.
- Mobile phones and other smart communication devices are governed by the school's separate Mobile Phone Policy.
- Breaches of this agreement may result in sanctions, temporary or permanent withdrawal of device privileges, restriction of network access, or safeguarding and disciplinary action where appropriate.

I understand that if I do not follow this agreement or a reasonable instruction from staff regarding the use of technology, I may be required to stop using, close, or put away my device. Continued misuse may result in confiscation, restriction of network access, temporary or permanent withdrawal of BYOD privileges, or safeguarding and disciplinary action where appropriate.

☐ Yes

☐ No

Appendix 2: Device Misuse Procedure

Device Misuse Procedure

Stage	Examples	Response	Further Action
Reminder	-Off-task browsing -non-educational websites -Device open when not required	Student asked to return to the task/close their device until instructed to use it.	-Student complies → no further action.
Final Warning	-Student resumes misuse.	Student informed that if they continue, the device will be confiscated until the end of the lesson.	-Recorded Behaviour note.
Temporary Confiscation	-Student refuses to comply after a final warning. -Continued misuse of the device.	Student instructed to stop and hand the device to the member of staff/place at the front of the classroom.	-Device retained until the end of the lesson. -Brief restorative conversation at the end of the lesson. -Recorded Behaviour note. -Parents informed.
End of Day Confiscation	-Repeated lesson confiscations. -Defiance towards staff instructions -Significant disruption caused through device misuse.	Device taken to Pastoral Director or Deputy Head Pastoral/Academic and returned at the end of the school day.	-Student informed that further incidents may result in loss of BYOD privileges. -Parents informed -Sanction in line with Behaviour policy.
Temporary Suspension of BYOD Privileges	-Multiple confiscations -Repeated failure to follow staff instructions. -Persistent off-task or inappropriate use.	First occasion: 1 week Second occasion: 2 weeks Third occasion: until end of the half term	-Parents informed. -Student must use alternative paper-based methods provided by teacher(s). -Sanction in line with Behaviour policy.

Permanent Withdrawal of BYOD Privileges	-Repeated misuse despite intervention. -Serious breach of trust. -Significant safeguarding, online safety, or cybersecurity concerns.	Process managed by Senior Leadership Team: Deputy Head Pastoral/DSL or Deputy Head Academic	-Parents informed. -External agencies informed where necessary -Sanction in line with Behaviour policy.
Immediate removal (no prior warning required)	-Safeguarding concerns -Cyberbullying or harassment -Unauthorised photography or recording -Sharing images or videos of others -Use of VPNs, proxies or personal hotspots -Accessing harmful, extremist or illegal content -Deliberate attempts to compromise network security -Serious AI misuse -Any behaviour placing others at risk	1)Senior Leadership Team called to classroom. 2)Device handed over immediately. 3)Investigation undertaken by Deputy Head Pastoral/DSL or Deputy Head Academic 4)Decision made regarding return, sanctions and continued BYOD access.	-Parents informed. -External agencies informed where necessary -Sanction in line with Behaviour policy.



GUILDHOUSE SCHOOL
LONDON



Creating tomorrow's change makers.