COGNITA

BRIGHTON COLLEGE
(SINGAPORE)

Acceptable Use of Technology Policy (Senior School)

DOCUMENT CONTROL

Version Control		
Author	Jonathan Snell, Head of Computing	
Version Number	00	
Effective date	Oct 2025	
Next review date	Oct 2026	
Changes from previous version	**RESPONSIBILITIES:** N/A **PROCEDURES:** N/A **APPENDIX:** N/A	
Previous Version	**Author**	**Effective Date**

1. Philosophy and Vision

Brighton College (Singapore) prepares pupils to thrive in a digital society with confidence, kindness, and curiosity. Technology is a powerful tool for learning, creativity, and connection. With this privilege comes responsibility: pupils must use all technology and systems thoughtfully, purposefully, and safely, always placing learning first.

This policy sets out our specific expectations for all Senior School pupils (Years 7–13) when using technology for school purposes. This policy applies to any technology use in school, when accessing our systems outside of school and when pupils are on school trips. By using our systems and by configuring your BYOD device for our infrastructure, you are agreeing to follow this policy and understand that unacceptable use will result in school taking actions outlined in the **Pupil Behaviour Policy**.

2. Learning & Digital Accounts

- Use technology in lessons only as directed by staff, and always for learning first.
- Only use your own username and password; never share or use another person's account.
- Inform your teacher or another trusted adult if you think someone else has your password and might be using your account.
- Do not install, download, or run unapproved software, apps, VPNs, proxies, or use personal hotspots to bypass school filtering/monitoring.
- You can access your School Account provided by Microsoft365 (and other accounts) from any device, but you must be aware that all digital activity within your school digital accounts is monitored and tracked.
- All of your School Accounts (including your Microsoft365 account) should only have your school photo used as the profile photo. No other photo is allowed.

3. Research, AI & Academic Integrity

- Check and evaluate sources; avoid plagiarism by crediting all materials used.
- Be transparent: declare how AI was used in your work and cite appropriately.
- Never submit AI-generated work as your own.
- Follow copyright and intellectual property law when using or sharing digital materials.
- GenAI should only be used by pupils in Year 9 and above.
- Pupils in Year 9 and above must follow the specific rules and guidance when using Generative AI that has been outlined in our **Academic Integrity Policy**.

4. Communication & Conduct

- Communicate online with respect: all messages, posts, and emails must be polite, responsible, and on approved platforms.
- Never create, share, or forward bullying, discriminatory, hateful, or humiliating content including on group chats, gaming environments, or social media. This rule should be followed inside and outside of school hours.
- Do not impersonate others or create fake accounts.
- Model kindness, empathy, and integrity in all digital interactions.
- Uphold our school values in all digital spaces, inside and outside of school.
- Do not use any personal accounts for school-related communication. Always use the school provided account within the Microsoft 365 environment.
- The school implements a 6pm-6am rule for emails. Which means that no emails should be sent between these times. If you are writing an email at this time, please use scheduled send so it can arrive within allocated hours for the recipient.

5. Images, Audio & Video

- Always gain consent before photographing, filming, or recording anyone.
- Do not share any images, audio, or video that you have recorded other than for the intended purpose.
- During the school day, only capture images, audio and video that are linked to a learning task.
- Do not access personal photos, videos or audio on your BYOD device during the school day.
- You must store images, audio and video for learning in the correct way as directed by your teachers.
- Never create, request, view, or share explicit or harmful images. This is illegal and a serious safeguarding issue which will be reported to our safeguarding team and the appropriate law enforcement agency.

6. Devices & BYOD

- Our BYOD Programme requires all devices to be setup by IT Services and attached appropriately to our school network. You must have this process completed by IT Services before using your BYOD device.
- Keep your BYOD device safe, secure, and charged and bring your charger to school with you.
- Do not connect unknown USBs, accessories, or external drives to your BYOD device.
- Do not hotspot or use mobile data to avoid filtering.
- Report viruses, malware, or suspicious activity at once to IT Services.

- Store all your data in your School Account provided by Microsoft 365. Data saved on your desktop or in the local documents folder will not be backed up.
- Your mobile phone, smart watch or any other personal electronic device should be handed in to your tutor every morning and collected at the end of the day during tutor time. The only digital device allowed during the school day is your BYOD device and headphones when directed by the teacher.
- Keep your BYOD device in good working order and respect school-owned equipment.
- Restart your BYOD device every morning and close any personal apps so you are ready for learning.
- During the school day, no messaging applications should be used other than those provide within your Microsoft 365 school account.

7. Digital Etiquette and Classroom Expectations

- Value human interaction: devices down by default unless instructed.
- Follow teacher instructions on when and how to use your BYOD device and any other technology in the classroom.
- Focus on learning: social gaming, social media, personal music or videos are not allowed during school hours and will result in your device being confiscated for a fixed time and your parents being contacted as outlined in the pupil behaviour policy.
- Keep an "open screen" policy. No hiding tabs, desktops, or activities.
- During assessments, comply fully with exam regulations, including secure use of technology.
- No headphones should be used unless they are needed as part of the learning and have been instructed by the teacher.

8. Online Safety – The 4Cs

- **Content (What you see):** Do not access or share illegal, harmful, or inappropriate material (e.g., pornography, racism, self-harm, extremism, disinformation). If you encounter it accidentally, stop, block, and report it to a teacher or a trusted adult.
- **Contact (Who you talk to):** Be cautious in online communication. Do not share personal details or meet online contacts without parental and school knowledge. Report unwanted or unsafe contact at once to a teacher or to a trusted adult.
- **Conduct (How you behave):** Do not bully, harass, discriminate, hack, spread malware, or bring the school into disrepute. Never take part in dangerous online challenges. Report any incidents of this to a teacher or a trusted adult.
- **Commerce (Money & scams):** Avoid gambling, unauthorised purchases, scams, and phishing. Report suspicious requests for payment or personal details to a teacher or a trusted adult.

9. Monitoring, Reporting, and Sanctions

- All network and device use is filtered and monitored during the school day.
- All activity using school accounts is monitored whenever and wherever it is used.
- Safeguarding staff will review activity to protect individuals and the community.
- As part of our school values, we would expect pupils to report concerns promptly to a teacher, trusted adult, or a member of the safeguarding team.
- Breaches of this policy will be actioned in line with the **Pupil Behaviour Policy** and our **Safeguarding Policy**, and may result in:
- loss of access to devices/networks
- restorative actions or disciplinary measures
- parental contact
- where necessary, referral to external authorities

RELATED LEGISLATION AND DOCUMENTS

- Academic Integrity Policy
- Pupil Behaviour Policy
- Safeguarding Policy

APPROVAL DETAILS

Approved by:

Academic Board Approval, if applicable Name: Date:	Head of College Name: Nicholas Davies Date: Oct 2025

CAH Approval, if applicable

CEO Name: Date:	COO Name: Date:	CFO Name: Date:

DOCUMENT HISTORY

Date	Version		Author	Description	Reviewed by/Date	Effective d
Sep 2025	00		Jonathan Snell	Initial Implementation	Nicholas Davies	Oct 2025