BHASVIC

ACCEPTABLE USE OF IT POLICY FOR STUDENTS

Last Updated: September 2026

Review Date: September 2029

BHASVIC

BHASVIC Acceptable Use of IT Policy for Students

Your Digital Use Charter

Be Resourceful. Be Responsible. Be Respectful.

Use your BHASVIC account for college work — keep it private and secure.
Save your work in OneDrive or Teams, where it's backed up and safe.
Use AI to support not replace your learning and always be open about how you've used it.
Keep your device updated and locked; connect to college Wi-Fi via eduroam.
Treat others with respect online and offline.
If something feels unsafe, speak to a trusted adult or the Safeguarding Team.

1. Your BHASVIC Account

Your BHASVIC account gives you access to Microsoft 365 (Word, Excel, PowerPoint, Teams, Outlook, OneNote, OneDrive), college systems, and eduroam Wi-Fi. Use it well and it will serve you well throughout your time here.

Keeping your account safe

Use your own login — don't share it with anyone.
Choose a long password (three random words works well) and don't reuse it on other sites.
The college requires you to use an authenticator app to protect your account. Enable two-factor authentication (2FA) when asked — it acts as a second key to your account. It protects you if your password is ever stolen.
If you think someone else has access to your account, change your password straight away and tell IT Helpdesk.
You agree to complete any online safety or cybersecurity training the college requests of you.
Your account access ends when you leave BHASVIC (31 August of your final year). Make sure you've saved anything you need before then — accounts are deleted shortly after.

Your Microsoft 365 licence

Your college account gives you access to the full versions of Microsoft tools. These are available as web versions, as well as downloadable apps. You can install Microsoft 365 Office on up to 5 of your own devices — download it from Microsoft 365 Office (https://www.microsoft.com/en-us/microsoft-365/download-office) using your BHASVIC email.
This includes Word, Excel, PowerPoint, Teams, Outlook, OneNote, and OneDrive.
All users receive online storage in OneDrive. The college has the right to adjust your storage limits, as well as restrict your access to your account if you exceed your storage limit.

2. Using AI

AI is a powerful learning tool when used thoughtfully. BHASVIC encourages you to explore AI to deepen your understanding — research ideas, generate revision aids, test your knowledge with quizzes, and practise scenarios. Don’t let AI do the thinking for you.

Using AI well

Use Microsoft Copilot, signed in with your BHASVIC account — it's the AI tool provided for your studies.
Treat AI outputs as a starting point: verify facts, question assumptions, and develop ideas in your own words.
Record what you used: the tool name, date, and how it helped you. Screenshots are useful evidence of AI use for coursework.
Follow your teacher's guidance on when and how AI can support specific assignments.

Academic integrity

If AI has contributed to your work, say so.
Include:

- The tool you used (e.g. Microsoft Copilot)
- The date
- How you used it
- A screenshot of your prompt and output

Submitting AI-generated work as your own without declaring it is academic misconduct and may lead to penalties under JCQ and College rules.
See the Student AI Guide and JCQ AI Guidance (https://www.jcq.org.uk/exams-office/information-for-candidates/) for full details.

3. Your Device

You are required to bring your own device to college. A modern laptop gives the best experience, but any up-to-date laptop, Windows, Mac, Chromebook, or tablet will work well with college systems. Smartphones aren't adequate for classwork or homework.

Getting the most from your device

Bring it fully charged and ready to use. Lockable charging cabinets are available if you need a top-up during the day.
Connect to the internet via **eduroam** — this is the college Wi-Fi for students.
Keep your device updated and use a screen lock or biometric unlock.
Install Microsoft 365 from Microsoft 365 (https://www.microsoft.com/en-us/microsoft-365/download-office) using your BHASVIC account — it's free for the duration of your course.

Looking after your device

You're responsible for the security of your own device. Keep it safe, use a protective sleeve, and consider insurance.
Report any theft to the college security team immediately. The college is not liable for loss, damage, or theft of personal devices.

Loan devices

If you receive a financial bursary, you'll be offered a long-term loan of a college-owned device for your studies. Return it to IT by 30 June of your final year, in good working order.

Short-term laptop loans are available from self-dispensing cabinets, subject to availability. Return them on time and plugged in so they're charged and updated for the next person. Repeated failure to do this will result in loss of access to loan devices. These devices are not intended to be a replacement for having your own device. They are for short term emergency use.

Look after the laptops as if they were your own. You may be billed by the college for any loss or damage to a device while checked out in your name.

Connecting your device to college systems

To access the internet on campus, you'll connect via **eduroam**. Connecting to **eduroam** will install a network profile and security certificate on your device. This is what allows your device to authenticate on the network, and it also means your internet use on campus is filtered and monitored through **Lightspeed**, our online safety platform.

This filtering and monitoring apply **only while you're on the college network** — it doesn't follow you home or affect your personal internet connection. The profile is removed automatically when you leave BHASVIC, or you can remove it yourself.

College data on your device

When college applications (such as Microsoft 365) are installed on your personal device, the college uses Mobile Application Management (MAM) to keep college data separate from your personal data.

This means the college can remotely remove college data (emails, files, app access) from your device if needed — for example, when your account is closed when you leave, your device is lost or for safeguarding or security reasons. **This only affects college data.** Your personal photos, messages, apps, and files are never touched.

4. Online Safety and Respect

The internet is filtered and monitored on all college systems through **Lightspeed** to keep you safe and protect the college network. Monitoring is there to safeguard you, not to restrict your learning. To keep you safe, we ask that you do not attempt to bypass our security systems or access college resources via a VPN.

Using the internet well

If a site you need for your studies is blocked, ask IT to review it — requests go to the Online Safety Group.
Use college email and Teams for college communications. Report anything suspicious (phishing, unusual requests, unexpected attachments) to IT Helpdesk.
Be respectful online — the same standards apply as in person.

Where to get help

If something online makes you feel unsafe, uncomfortable, or worried, talk to your Tutor, the Safeguarding Team in Student Services, or any trusted adult in college.
If you're concerned about someone else's safety, do the same. Speaking up isn't telling tales, it's looking out for each other.

Please be aware

Online behaviour that amounts to bullying, harassment, or sharing harmful content is taken seriously and may lead to disciplinary action under the Student Behaviour Policy and UK law (including the Online Safety Act 2023).
Using technology to harm, harass, or exploit others — including creating, sharing, or possessing

inappropriate or illegal content, or seeking to gain unauthorised access to systems or data — is misuse of college IT and will be treated seriously. This includes the use of AI tools to generate harmful content or probe systems for vulnerabilities. This list is an example, not exhaustive: misuse is misuse, regardless of whether a specific scenario is listed here. Such behaviour will result in a safeguarding response and may be referred to external agencies including the police.

5. Mobile Phones

Mobile phones are part of everyday life, and at BHASVIC we treat them as a professional tool — something you use purposefully, not something that distracts you or others from learning.

Use your phone when it supports your learning, with your teacher's permission — for example, to research, photograph a whiteboard, or access an app your class is using.
During lessons and study periods, phones should be away unless you've been asked to use them. The default is focused work, not scrolling.
If you need to take a call or respond to something urgent, step out with your teacher's permission.
During break and lunch, and in social spaces, phones are fine — just be mindful of the people around you.
Headphones are for personal listening, not for during class unless your teacher has specifically allowed it.

6. Saving and Sharing Your Work

Save your college work in **OneDrive**— it's secure, backed up, and accessible from anywhere.
Avoid USB sticks and personal cloud storage (Google Drive, Dropbox, etc.) for college work — they aren't covered by the college's data protection arrangements. Share files as links rather than attachments. This allows you to revoke or modify access if needed.
For security reasons, your account is not accessible from overseas or through VPNs.
Remember: when you leave BHASVIC, your account and its contents are deleted. Save what you need before 31 August of your final year.

7. Monitoring and Enforcement

All BHASVIC accounts and activity on college systems are monitored for safeguarding, security, and compliance. This includes AI activity on Copilot when logged in with your BHASVIC account.

Serious misuse of college IT systems or online behaviour that puts others at risk may lead to disciplinary action under the Student Behaviour Policy, up to and including exclusion. In some cases, misuse may be reported to awarding bodies or the police.

Where to Get Help

What you need	Who to contact
Technical support (Wi-Fi, accounts, devices)	IT Helpdesk — Room 126 or ithelpdesk@bhasvic.ac.uk
Safeguarding concern	Safeguarding Team — see Student Dashboard or Student Services
AI guidance	Student AI Guide (https://bhasvic.sharepoint.com/sites/bha-Home/SitePages/StudentDigital-Induction.aspx#bhasvic-ai-student-guide)
Exam rules on AI	JCQ AI Guidance (https://www.jcq.org.uk/exams-office/information-for-candidates/)
Financial support for a device	See Student Services about bursary eligibility

Related policies:

This policy works alongside the Student AI Guide, Safeguarding Policy, Exams & Assessment Policy, and Student Behaviour Policy. Full college policies: bhasvic.ac.uk/the-college/policies

Version: September 2026
Next Review: September 2029
Status: Draft — replaces Student Acceptable Use Policy (Sep 2025) and BYOD for Students Policy (Jun 2023)