WELLINGTON COLLEGE BELFAST

Bring Your Own Device (BYOD) Policy for students

Introduction

The College recognises that mobile technology offers valuable benefits to students from an accessible learning perspective. Our College embraces this technology but requires that it is used in an acceptable and responsible way, in line with our existing College teaching and learning objectives.

This policy is intended to address the use by students, of non-college owned electronic devices to access the Internet via the site wide C2K managed wireless provision. Any mobile device with Wi-Fi capability is covered by this policy.

This policy is supported by the C2K Acceptable Use Policy, College E-Safety Policy, and Mobile phone policy.

Policy statements

1. Use of mobile devices at the school

Students must only use mobile devices as part of a planned lesson with prior staff permission, or during their timetabled study periods.

Students are responsible for their mobile device at all times, this includes whilst travelling to and from the College, inside the College, and whilst taking part in any College related activities. The College is not responsible for the loss, or theft of, or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. College reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

Devices must be fully charged when being brought to the College. No charging facilities are available as personal chargers must not be used due to the Portable Appliance Testing (PAT) requirement.

Mobile devices must be turned off when in a prohibited area and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply.

The College reserves the right to refuse students permission to use their own mobile devices on school premises.

2. Access to the College wireless Internet connection

The College provides a site wide wireless network that students may use to connect their mobile devices to the Internet. Access to the wireless network is at the discretion of the College, and the College may withdraw access from anyone it considers is using the network inappropriately.

The College cannot guarantee that the wireless network is secure, and students use it at their own risk. In particular, students are advised not to use the wireless network for online banking or shopping. It is available for educational purposes only.

The College is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the College's wireless network. This activity is taken at the owner's own risk and is discouraged. The College will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the College's wireless network.

3. Access to College IT services

Students are permitted to connect to or access the following C2K managed IT services from their mobile devices:

- The C2K provided email system
- The College virtual learning environment (Internet Explorer, Google Classroom, Office 365, and C2K Files)
- Apps as recommended by staff to facilitate teaching

Students must only use the IT services listed above (and any information accessed through them) for work & educational purposes. Students are only permitted to use their devices via connection to the C2K Wireless network, and are not permitted to use their mobile data, nor enable a personal wireless hot spot connection facility for themselves or others.

Students must use the C2K provided email account, and not use the C2K provided wireless network to access their personal email accounts.

All personal files, such as photographs, videos, and text messages must not be accessed on the mobile device within the College. Apps deemed unsuitable for use in the College must be removed prior to connection, or mobile device use. Lock screen and device wallpaper images must be suitable for use within the College environment.

If in any doubt the user should seek clarification and permission from the College IT Support technician before attempting to gain access to a system for the first time. Students must follow any written procedures for connecting to the school systems.

4. Monitoring the use of mobile devices

The College, and our managed system provider uses technology that detects and monitors the use of mobile and other electronic or communication devices, which are connected to or logged on to our C2K wireless network. By using a mobile device on the College's IT

network, students agree to such detection and monitoring. This is for the purpose of ensuring the security of its IT systems and for tracking school information.

The information that the College may monitor includes (but is not limited to) the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded to or downloaded from websites and College IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

5. Security of student mobile devices

Students must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Students must never attempt to bypass any security controls in school systems or others' own devices.

Students are reminded to familiarise themselves with the school's e-safety and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behaviour online.

Students must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

Students are advised to have a device tracking facility enabled on the device, where available.

6. Support

The College cannot support users' own devices but will offer advice to users in their use where practically possible; nor has the College a responsibility for conducting annual PAT testing of personally-owned devices.

7. Compliance, Sanctions and Disciplinary Matters for students

Non-compliance of this policy exposes both students and the College to risks. If a breach of this policy occurs the College may discipline students in line with the College's Disciplinary Procedures. Guidance will also be offered to students to support them in complying with this policy. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on College premises will be temporarily withdrawn. For persistent breach of this policy, the College will permanently withdraw permission to use user-owned devices on the network.

The College reserves the right to check any student mobile device for unsuitable content, or to investigate reports of BYOD misuse. This may include requesting an Internet browsing report from the Wi-Fi managed service provider.