ELEARNING POLICY

1.1.1. CLIFTON LOCAL AREA NETWORK

1.1.1.1. GENERAL PRINCIPLES

1.1.1.1.1. For the purposes of this policy, the term 'IT Device' is deemed to include tablets; iPads; notebooks; computers; laptops; cellphones and smartphones.

1.1.1.1.2. The Clifton Code of Conduct regulates the use of IT facilities, equipment and devices. Any contravention of this policy and the rules contained therein may lead to confiscations, detentions, warnings, disciplinary hearings and possible expulsion.

1.1.1.1.3. Food and beverages may not be eaten near or around the IT Devices or taken into any IT Room **under any circumstances**

1.1.1.1.4. It is expected that IT Devices be used as educational tools during lessons. Just as textbooks, pens and notepaper are viewed as necessary or useful in lessons, so the use of IT Devices should enjoy similar regard from the academic staff.

1.1.1.1.5. All IT Devices on the campus must be registered with the network and will be logged to a particular pupil. Any attempt to access the network outside of this arrangement equates to entering the school premises without permission and will be dealt with as such.

1.1.1.1.6. During class or any other supervised time, teachers may monitor pupils' activities and check application activity such as the use of a calculator or a dictionary, where these are deemed to be inappropriate.

1.1.1.1.7. All IT equipment and IT Devices must be treated with respect.

1.1.1.1.8. Only authorized Clifton pupils will be allowed to use Clifton IT Devices, and be logged on to the Clifton network.

1.1.1.1.9. Pupils may not log on to the network as an 'Administrator' at any time.

1.1.1.1.10. The use of any recording equipment (including photographs and film) provided by an IT Device is prohibited, unless specifically permitted and supervised by a teacher.

1.1.1.1.11. Restrictions may be applied at the discretion of the Executive Headmaster or his designate to the use of pupils' IT Devices on the Clifton network.

1.1.1.1.12. All pupils must log off from any IT Device immediately after use.

1.1.1.1.13. Computer games as well as other programs and applications, which are not specifically permitted, are not allowed on the Clifton Network unless they have been approved in advance by a Network Administrator.

1.1.1.1.14. Pupils may not engage in any form of cyber bullying.

1.1.1.1.15. All data on the Clifton School network is the sole property of Clifton School and can be viewed or accessed at any time by the Clifton School Network Administrators.

1.1.1.1.16. All work must be saved to iCloud, Dropbox (www.dropbox.com) or an equivalent for backup purposes. Clifton School cannot be responsible for loss of work as a result of hardware or software failure.

1.1.1.2. HARDWARE

1.1.1.2.1. IT Devices may not be shared without the consent of the pupil who has brought the IT Device to school. The IT Device must stay in sight, and under the control of the owner at all times.

1.1.1.2.2. IT Devices that belong to Clifton must be issued formally to pupils and pupils must sign for receipt (or the equivalent electronic acceptance). These devices may not be removed from the campus under any circumstances.

1.1.1.2.3. Where a device is broken by a pupil, it becomes the pupil's responsibility to replace it.

1.1.1.2.4. The Clifton management reserves the right to refuse a pupil the use of an IT Device, should that pupil abuse the device or contravene the elearning policy.

1.1.1.3. SOFTWARE

1.1.1.3.1. No unlicensed software may be installed on a device, laptop or computer that is used on the school premises.

1.1.1.3.2. No preinstalled Clifton School software may be uninstalled or disabled.

1.1.1.3.3. Software installed by the Network Administrator is controlled from the Clifton College and Clifton Prep Media Centres and needs to be issued from these facilities, according to the procedures followed for book issues.

1.1.1.3.4. Software-related problems should be reported to the Network Administrator via the helpdesk facility on the Clifton network.

1.1.1.4. SECURITY

1.1.1.4.1. Clifton School and the staff of Clifton take no responsibility and accept no liability for the loss of IT Devices whether used at the School or while on school activities. This includes those periods when the IT Devices are held in confiscation, as a result of a failure to follow the Code of Conduct.

1.1.1.4.2. No boy may be in a computer room unless a member of staff is present or unless he has permission from a member of staff.

1.1.1.4.3. Where IT Devices are required for academic use, they should always be kept secure and remain the responsibility of the pupil. Security settings on the IT Devices should be set to allow for tracking and, where applicable, disabling them.

1.1.1.4.4. All passwords must be kept confidential.

1.1.1.4.5. Pupils are not permitted to access or attempt to access private or secured data.

1.1.1.4.6. Pupils are not permitted to log on to the Clifton Local Network on behalf of another pupil.

1.1.1.4.7. Pupils are not permitted to have any hacking software or documentation in their possession, installed on their IT Devices or have such software or documentation running on an IT Device.

1.1.1.4.8. Attempts to hack the network, its peripherals and servers will be viewed as a serious offence under the Code of Conduct.

1.1.1.4.9. When not in use, IT Devices should be closed, locked and, where possible, out of sight to any third party, locked away securely in lockers or be handed in at the front office for safe keeping. Those handed in must be collected at the end of the day.

1.1.1.4.10. All IT Devices must be switched off (not merely set to silent) during any school activity where they are not required. These activities include, without limitation, sporting activities and matches, assemblies, hymn practices, clubs, societies and school outings.

1.1.1.4.11. IT Devices are not permitted on, nearby or in the possession within the classroom of a boy who is writing a test or examination. The only exception to this is where the pupil has the permission of a teacher. Pupils should hand any IT Devices to the teacher prior to the start of the test or examination. If an IT Device is found on a pupil while he is writing a test or an examination, a presumption of cheating will arise and a staff member will be entitled to confiscate the IT Device pending disciplinary action against the pupil. This is viewed as a serious offence.

1.1.1.5. E-MAIL AND INTERNET ACCESS

1.1.1.5.1. Use of the Internet is restricted to academic purposes. Pupils may not use the Internet before school and at breaks.
1.1.1.5.2. The Internet may only be used with the express permission of a teacher.
1.1.1.5.3. Social media sites may not be accessed, unless with the permission of a teacher.
1.1.1.5.4. Printing may only be done under the supervision of a teacher and, where appropriate, a charge may be levied.
1.1.1.5.5. Security levels and computer settings may not be altered.
1.1.1.5.6. Pupils are not permitted to visit any undesirable, unsuitable or pornographic websites at any time, or forward such material to anyone. If any such site is found or any such email is received from the Internet, pupils are to notify the Network Administrator immediately
1.1.1.5.7. Pupils are not permitted to download files or software from the Internet that are unrelated to study or research. **Downloading includes watching videos from the Internet and browsing and saving pictures, files and software from the Internet.**
1.1.1.5.8. Pupils must request permission from the Network Administrator to download relevant files and software from the Internet and should take care not to duplicate material that has been downloaded previously. Pupils may not send chain letters or bulk mails via the network.
1.1.1.5.9. Personal email may not interrupt normal duties and should only be accessed during official breaks or free periods.
1.1.1.5.10. Pupils may not send abusive, undesirable or unsuitable email.
1.1.1.5.11. Pupils may not send mail messages larger than 2 MB in size.
1.1.1.5.12. We run an open network and pupils may not attempt to hide or otherwise avoid the School's ability to monitor their safe use of technology. This includes VPN software, Jailbreaking and Cydia, TOR browsing or any similar products or protocols

1.1.1.6. RESTRICTIONS

1.1.1.6.1. All iPads in Grades 4 to 7 must be restricted and special internet browsing software must be installed. Instructions about how to do this will be made available to parents and pupils and can be found on our website.
1.1.1.6.2. Clifton strongly discourages pupils in this phase to be involved with social media (Facebook, Instagram, Whatsapp, Snapchat, Facetime and any similar products) unless this is strictly monitored by parents who are willing to take responsibility for any issues that may arise. Clifton cannot monitor or control private companies and platforms and will only accept responsibility for issues arising from apps that are recommended by Clifton.
1.1.1.6.3. Clifton cannot accept any liability or responsibility for activities or incidents that occur outside of school hours and particularly if these occur using Apps that are not sanctioned by the School, if restrictions have not been correctly applied and/or if pupils have been given access to make purchases or change settings on their accounts.

1.1.1.7. SANCTIONS

1.1.1.7.1. Failure to comply with any of the above requirements will result in the following sanctions:
- For an offence deemed to warrant a disciplinary hearing without warning - confiscation and a disciplinary hearing.
- First offence – one-hour detention.
- Second offence – a two-hour detention or the equivalent.
- Third offence – Saturday detention or confiscation and a disciplinary hearing.

(This document is compiled with grateful acknowledgement to the staff at Parklands College for making their policy available to us.)