DUBAI COLLEGE

A tradition of quality in education

Use of Information and Communication Technology

Students are provided with IT resources to optimise their learning. These resources come in 3 forms.

1. Online resources
2. Computer Laboratories
3. Access to wireless network via personal devices

Online Resources

Online resources can be remotely accessed via mydc.dubaicollege.org. Resources such as reports, wireless device registration, and files can be found at this link.
Online resources are found on network share drives. Students have the OneDrive area for personal files and a subject SharePoint or OneNote area for shared resources such as subject-specific files.

Computer Resources

There are four computer laboratories for instruction. The four laboratories are used for timetabled ICT instruction but used by other subjects for the support of teaching and learning. The Library Pod and other associated computers are also available for student use. Sixth Form students have their own ICT suite as does Design and Technology.

Rules for the school computer labs are as follows.

1. Treat all ICT equipment with care.
2. Do not eat or drink in the ICT laboratories or Collaborative Learning Spaces
3. Use computers for school work only
4. Do not attempt to access another student's account
5. Do not tamper or interfere with the system
6. Do not download anything
7. Store all your work on your 365 cloud
8. Only use the Internet for school related work
9. If there is a problem with your computer, do not attempt to fix it yourself
10. Where they exist, follow the printing rules at all times; in essence do not print off multiple or unnecessary pages.

Access to Wireless Network

The school provides wireless access for students. To provide security for all users, the school implements several layers of security for wireless access. A student must first register their device before it is activated for use. The device may be registered on https://mydc.dubaicollege.org via the "myTools" link. IT staff can then activate the device for use.

IT Facilities

Users are encouraged to make use of the school's IT facilities only for educational purposes.

Personal Technology Use

- Technology should be used responsibly at all times.
- Users are responsible for the protection of their own devices and network accounts, they should not divulge their password to anyone. This includes classmates, parents, and teachers. Users should not log on to or use any account other than their own and should log off when leaving a workstation, even for a short period of time.

Use of Facilities

It is not acceptable to

- Attempt to download or install software to school computers.
- Attempt to introduce a virus to the network.
- Attempt to bypass network or system security.
- Attempt to access the account of another user.
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking/cracking software or system.
- Connect any device to the network that has access to the Internet via a connection not provided by the school.
- Access and download material that is indecent or obscene, infringes copyright, is unlawful, or brings the name of the school into disrepute.

Internet Access

- The school's Internet service is filtered to prevent access to inappropriate content and to maintain the integrity of the computer systems. Users should be aware that the school logs all Internet use. While the school respects the privacy of users, users should assume all of their activity could potentially be monitored by the school or others.
- The use of public chat facilities is not permitted.
- Users should not copy or use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by the examination boards.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.

Privately Owned Computers

Personal laptops and desktops are allowed to be connected to the school network. They are subject to the DC Acceptable Use Policy. All computers, for their own protection, must have antivirus software installed. This includes Macintosh machines. Peer to peer software may not be on the computers. This is to prevent network performance degradation, observe local and international laws, and to protect the network from intrusion as such software compromises the machine and the network.

Privacy and Personal Protection

- Users must, at all times, respect the privacy of others.
- Users should not forward private data without permission from the author.
- Users should realise the school has a right to access personal areas on the network.
- Privacy will be respected unless there is reason to believe that the Acceptable Use Policy has been breached or that school guidelines are not being followed.

Disciplinary Procedures

The Acceptable Use Policy constitutes part of the school's Behaviour and Sanctions Policy.

Those who misuse the IT resources or violate the Acceptable Use Policy will be subject to disciplinary procedures. Violations may result in disciplinary action up to and including suspension or expulsion for students. When applicable, law enforcement agencies may be involved after consultation with the KHDA.

Policy Details	
Version date	December 2020
Last review	October 2019
Next review	September 2021
Responsible SLT	Deputy Head Learning and Teaching