

## Acceptable use of ICT services, facilities and devices

Students at Cleveland District State High School use Information and Communication Technologies (ICT) as an integral part of their learning and to equip them to live and work successfully in the digital world. Cleveland District State High School has an extensive network of digital infrastructure including student owned laptops, school owned laptops, desktop computers, data projectors, printers/copies/scanners, robotics equipment and a vast range of other digital equipment to support student learning.

At all times while using ICT facilities and devices at school, whether personal or school owned, students will be required to act in line with the requirements of Cleveland District State High School's Student Code of Conduct.

In addition students and their parents should:

- understand the responsibility and behaviour requirements (as outlined by the school) that come with accessing the department's ICT network facilities
- understand that a student-owned laptop used at school may only access the internet by connecting through the school's restricted network. Students must **not** access the internet via tethering/hot-spotting to cellular network technology ie: 3G/4G/5G enabled device.
- ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email
- be aware that:
  - access to ICT facilities and devices provides valuable learning experiences for students and supports the school's teaching and learning programs
  - the school is not responsible for safeguarding information stored by students on departmentally-owned devices, student-owned devices or mobile devices
  - schools may remotely access departmentally-owned student computers or mobile devices for management purposes
  - students who use a school's ICT facilities and devices in a manner that is not appropriate may be subject to disciplinary action by the school, which could include restricting network access
  - despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed
  - teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

## **Acceptable/appropriate use of ICT by a student**

It is acceptable for students while at school to:

- use personally owned laptops, or school owned devices for:
  - assigned class work and assignments set by teachers
  - developing appropriate literacy, communication and information skills
  - authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, their parents or experts in relation to school work
  - accessing online references such as dictionaries, encyclopaedias, etc.
  - researching and learning through the department's eLearning environment
- be courteous, considerate and respectful of others
- use their personal laptop device for private use before or after school, or during lunch breaks, in accordance with Student Code of Conduct.

## **Unacceptable/inappropriate use/behaviour of ICT by a student**

It is unacceptable for students while at school to:

- use any ICT device in an unlawful manner
- record images or video of students or school staff without their consent
- record images or video of the school grounds without the permission of the Principal
- publish any media online which includes students in school uniform, or involved in a school activity (example school sport, camps) without the permission of the Principal
- publish any media online which includes school staff or the school grounds without the permission of the Principal
- download, distribute or publish offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment, or stalking
- insult, harass or attack others or use obscene or abusive language
- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions regarding the use of social media, online email and internet chat
- send chain letters or spam email (junk mail)
- share their own or others' personal information and/or images which could result in risk to themselves or another person's safety
- knowingly download viruses or any other programs capable of breaching the department's network security
- use in-device cameras inappropriately, such as in change rooms or toilets
- invade someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- use digital technologies (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use electronic devices at exams or during class assessment unless expressly permitted by school employees.
- share network log-in details, or use another student/staff members log-in details to access the school network.