

# Student Cyber Safety Code of Conduct



THE KING'S COLLEGE  
Be exceptional.



## Compliance and Review

The King's College is committed to the continuous improvement of its Child Protection Programme and adhering to the WA child protection laws, regulation and standards.

The King's College  
Student Cyber-safety  
Code of Conduct

Reviewed by: The Principal

Endorsed by: The School Board

Updated: October 2019

Review: October 2020





# Student Cyber Safety Code of Conduct

## 1. Overview

The College computer network, Internet access facilities, computers and other College Network equipment/devices bring great benefits to the teaching and learning programmes of the school and to its effective operation. The Internet is an excellent resource for research and communication; however, there is material on the Internet that is objectionable and inappropriate for research or general use.

College Network equipment and devices can also be used in a manner that is detrimental to the individuals and the community. For these reasons there need to be measures put in place to guide the use of the Internet and network equipment at The King's College.

The College aim in this matter is to create and maintain a culture of Cybersafety. This culture of Cybersafety must be in keeping with College values as well as legislative guidelines and professional obligations.

The College Network is for educational purposes – for teaching and learning activities appropriate to the school environment. This applies to any College Network equipment used to access the College Network, whether it is owned or leased (either partially or fully by the college), utilised by a vendor or third party or is a privately-owned device.

## 2. Definitions

- The abbreviation *ICT* refers to the term Information and Communication Technologies.
- 'College Network' refers to the technical entity that is the ICT environment at the college and includes the platform that each student logs into.
- *Cybersafety* refers to the safe and secure use of the Internet and College Network equipment and devices.
- *College Network* refers to the College's computer network, servers, Internet access facilities, computers and other College Network equipment/devices as outlined below.
- The term *College Network equipment/devices* used in this Code of Conduct, includes, but is not limited to, computers (such as desktops, laptops, notebooks, netbooks, tablets and mobile phones), storage devices (such as USB and flash memory devices, hard drives, DVDs, iPods, MP3 players), servers, cameras (such as video, digital, webcams, all types of gaming consoles, video and audio players/receivers (such as portable CD and DVD players), network devices (such as wireless access points, switches and routers) and other similar technologies as they are developed and come into use.
- *Objectionable or inappropriate* means material that deals with topics such as sex, personal beliefs or violence in such a manner that is likely to be harmful to the wellbeing of students and/or incompatible with College standards and values. This type of material has no educational purpose in the College environment.

# Student Cyber Safety Code of Conduct

## 3. Student Cyber-safety rules for College students

### 3.1 The following rules apply to the use of College Network equipment/devices

- Students may use the College network after the Student Cybersafety Code of Conduct Agreement has been signed by both student and parent and recorded by the College.
- Every student has been issued with a personalised *username* and *password* for use of the College Network. Students may not use the *username* or *password* of another student.
- Students should not give their username or password to any other student or allow them to make use of these personal details.
- Students are not allowed to trespass in another student's folders, files or work.
- The College Network is provided for the educational purposes of each student and therefore wilful interference with the equipment, making it difficult or impossible for another member of the College to use, is prohibited. This includes the changing of settings, hacking, installation of malicious software or physically abusing hardware, leads, cables or other parts of the equipment/device.
- Students are reminded that they have access to their personal folder on the network as well as their Year group folder. Hacking is the attempt to gain access or the gaining of access to a site, file or folder that is not authorised to that student or person. (Even the attempt to access unauthorised sites is regarded as hacking.)
- Students are not permitted to use a network, device or software to disrupt the service of the College Network, or the individual use of the College Network by another student.
- Students are not permitted to use or access the computers or College Network equipment or devices of a staff member.
- Students should not use College Network, or their own personal College Network, to participate in any activity which may place themselves or another student at risk. This may include the use of e-mail, chatrooms, Facebook, Twitter and other social media sites.
- One of the main values of the College is respect, therefore the use of social media, electronic devices, College network equipment or mobile phones to deliberately harass, bully, offend, threaten or harm another student is prohibited by the College both during and outside College hours. This applies even if it is meant as a joke.
- The posting or communication of insulting, offensive, threatening and detrimental remarks or statements about the College, College staff, students, parents and community via social media and/or College Network equipment/devices is forbidden. This applies even if it is meant as a joke.

# Student Cyber Safety Code of Conduct

- The use of obscene language and swearing is forbidden in any communication using the College Network. This includes song, media and video recording, e-mails, graphics, printing and other forms of educational teaching and learning activities.

## 3.2 Whilst using the College Network

- Sending, displaying, accessing objectionable/inappropriate or age restrictive sites is prohibited.
- Downloading, saving or distributing material from such sites by copying, storing, printing or showing it to other people is forbidden.
- Attempts to bypass, circumvent, or get around security, filtering and monitoring in place at the College is not allowed.

## 3.3 Personal ICT equipment

- Students who bring their own ICT equipment to the College are under the same restrictions as those already outlined. Material and images on privately owned ICT equipment must follow College guidelines and be appropriate for viewing and listening on the College grounds or whilst on supervised College activities.
- Students may not download files such as videos, games or programs without the express permission of a teacher.
- The uploading of files such as videos, games or programs onto the College Network is also forbidden without the express permission of a teacher.
- All damage, breakages, misuse and irresponsible treatment of the College Network must be reported to a staff member immediately.

## 4. The Law

4.1 Students are reminded that there are state, federal and international laws in place that govern the use of all ICT equipment.

- The transmission of any material in violation of state, federal and international regulations is prohibited.
- Software piracy is illegal.
- The violation of copyright laws when researching is also illegal. Material from the Internet, DVDs, CDs, videos and other pieces of information created by another person must be carefully and correctly cited in research.

## 5. General rules

5.1 Using the College Network for profit, product advertisement or political lobbying is prohibited.

5.2 All students should respect the intellectual property and privacy of others.

5.3 The breaking of these rules will result in parents/guardians being informed and disciplinary

# Student Cyber Safety Code of Conduct

action being taken.

5.4 If an offence is in violation of the law, outside agencies such as the police will need to be informed.

5.5 Students must also realise that in the event of wilful destruction, damage or defacement of College Network equipment or devices, their family may be charged for repair or replacement costs.

**It is important for students to understand that staff have the right to access student files as they are for educational purposes only and therefore will be inspected by teachers and administration.**

## 6. Student Cybersafety Conduct Agreement

The *Student Code of Conduct Agreement* (Appendix 1) outlines the basic agreement between students and the College. Parents also sign this agreement as witnesses of their child's intended behaviour. Once this agreement is signed and recorded at the College, students will be able to use the College Network equipment and devices.

**The Cyber-safety Conduct Agreement is set out in full in the College's Student Diary.**

### 6.1 Please sign and return to Reception

I (*student name*) \_\_\_\_\_ have read and understand the College Code of Conduct for Cyber-safety. I agree to and abide by all conditions and guidelines of the Cyber-safety Code.

\_\_\_\_\_

**Student Name**

\_\_\_\_\_

**Student Signature**

\_\_\_\_\_

**Date**

\_\_\_\_\_

**Parent Signature**

\_\_\_\_\_

**Date**

#### ***Related Policies and Information:***

*ICT and Internet User Policy*  
*Behaviour Management Policy*  
*Student Code of Conduct*  
*Family Handbook*  
*Student Diary*