Acceptable Use of ICT (Information Communication Technology) Systems and ICT Infrastructure Policy

Policy Classification		
Policy Number:	Date of Origin: May 2014	By Whom: Senior Leadership Team
Policy Audience: Public Domain	Review Dates: June 2016, Mar 2019	Next Review Date: 2021
Policy Approval: This policy was approved by the Principal and Senior Leadership Team in March 2019		
This policy supersedes all previous policies in relation to matters contained herein.		

1. Rationale

1.1 The purpose of the policy is to ensure all staff and students are aware of their responsibilities when using ICT Systems and ICT including information security and data breach (Please also refer to the Information Security Policy)

1.2 All staff and students must follow the relevant guidelines at all times. Staff and students are responsible for their behaviour and actions when carrying out any activity which involves using Oakhill College's ICT Systems and ICT Infrastructure either within the College or at other locations, such as home.

1.3 ICT Systems and ICT Infrastructure includes all facilities and resources used to access the College ICT network, internet and infrastructure including standalone devices with digital storage.

2. Guiding Principles

The following principles outline the minimum standards required when using the College's ICT Systems and ICT Infrastructure that users are required to comply with.

2.1 This policy applies to all students and College employees including casual, temporary and contract staff.

2.2 This policy applies to both College supplied and personal (BYOD) devices accessing College services or systems including network and email.

2.3 The implications and personal responsibilities in relation to the use of ICT resources as detailed within this policy need to be understood and agreed by all users.

2.4 ICT resources must be accessed through the allocated username and password only. Username and password combinations must be kept secure. Users are required to log out after each session and never allow other users to access the internet or ICT resources with their username and password.

3. Policy

3.1 Communication devices and associated services, including telephones, mobile phones, computers, tablet devices, personal digital assistants, facsimiles, Internet, Intranet, email and broadband data services are resources provided for official purposes, and all employees have a responsibility to ensure their proper and secure use.

3.2 Employees and students must at all times comply with State and Federal laws relating to the use of communication devices. Using the College's communication devices to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Employees or students who do so may find themselves subject to criminal proceedings and or disciplinary action.

3.3 Employees or students must not engage in any use that may be considered questionable, controversial, offensive, or could potentially damage the College's reputation. Employees must adhere at all times to the College's Code of Conduct Policy and students must comply with the Acceptable Use of Mobile Phones and Smart Devices policy and guidelines and ICT Infrastructure Usage which are found in the College Diary and which the students sign as having read. Failure to do so may result in disciplinary action.

3.4 Employees provided with communication devices are advised that the use of those devices may be monitored to ensure compliance with this policy. Monitoring will comply with the NSW Workplace Surveillance Act 2005 and the College Surveillance Policy.

3.5 Student files, communication and internet activity will be monitored and checked. Students should be aware that a breach of this policy may result in disciplinary action in line with the College Discipline Policy.

3.6 Users must not attempt to interfere with or maliciously use a device that is the property of another staff member or student.

3.7 Any filtering and/or security systems put in place by Oakhill College must not be bypassed or attempts made to do so.

3.8 When an ICT resource has been damaged or affected by a virus or other malware, it needs to be reported to the Oakhill Helpdesk immediately.

3.9 Oakhill College ICT Systems or Infrastructure must not be used to:

a) Abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other means)
b) To send, receive, view or download inappropriate or pornographic material
c) Harm the reputation of Oakhill College in any way
d) Perform any unlawful or inappropriate act

3.10 Users must not download, install or run any software from the internet or from any other media which may compromise or interfere with the Oakhill College ICT Systems and Infrastructure.

3.11 College-owned equipment that is taken off site (Home/ College trips), such as laptops, tablets, cameras, removable media or phones, must be stored securely when not in use.

3.12 College-owned ICT equipment needs to be returned to a member of the ICT Helpdesk Team once it is no longer required.

3.13 Access to any document that contains personal information relating to other students or staff must be protected.

3.14 Any suspicion or evidence of unauthorised access or disclosure of personal information, or the loss of personal information (e.g. loss of equipment containing personal information) must be reported to the Oakhill College Helpdesk immediately. (Please refer to the Oakhill College Information Security Policy for further detail in regard to data breaches and mandatory reporting of data breaches)

3.15 Any content or communication that is unpleasant or upsetting, or is believed to be illegal, or could be considered offensive by another user must be reported to a senior member of staff or ICT department immediately.

3.16 Users must not intentionally damage, disconnect or interfere with any College-owned ICT equipment or infrastructure.

3.17 Users must not eat or drink while using Oakhill College Computer Labs or loan ICT Equipment.

3.18 Users must take personal responsibility for their own data. Any data stored locally on a mobile device will need to be backed up by the user. Oakhill College does not accept any responsibility for any data that is lost as a result of a failure to back up all items.

Social Media

3.19 Users need to take reasonable precautions to protect the personal information contained on social networking sites.

3.20 STUDENTS are only allowed to use social networking sites within College hours with explicit permission from a teacher.

3.21 Users must maintain a positive online identity, both in and outside of the College, and not abuse or attempt to cause offense to any member of staff or pupil via any comments, video, text or audio. Users must not make any comments about Oakhill College which could potentially damage its reputation.

3.22 Users must not give away any Oakhill College related personal information or the personal information of other users in the Oakhill College community over the internet except in circumstances governed by the College Privacy Policy and the Australian Privacy Principles. This includes but is not limited to photographs or videos of themselves, other pupils or members of staff.

3.23 STUDENTS must not arrange to meet someone they have met online unless this is part of College work, in which case they must arrange a responsible adult, parent or guardian to go with them.

3.24 When any offensive or hurtful comments relating to Oakhill College, members of staff or students are experienced online, screenshots for evidence must be taken and the incident must be reported to a member of the pastoral care team, teacher or the ICT Helpdesk.

Managing Digital Content

3.25 Safe and responsible behaviour must be demonstrated when accessing, creating, sharing and storing digital content (e.g. images, video and audio).

3.26 Digital content (e.g. images, video and audio) must not be created without the permission of any participants contained within the content.

3.27 Digital Content (e.g. images online) must not be published or shared without the permission of the staff and/or pupils involved in the content.

3.28 When using Digital Content, users must ensure that they are not in breach of any copyright law and ownership of online sources must be respected and acknowledged

3.29 STAFF - Oakhill College is the owner of all intellectual property uploaded, sent and created using Oakhill College ICT Systems and Infrastructure.

Email

3.30 Users must use their Oakhill College email address for Oakhill College related matters only.

3.31 Users must take care in opening any attachments sent by email. Emails and associated attachments must only be opened when received from trusted senders.

3.32 When sending emails, users must ensure that they are respectful and professional and Oakhill College email accounts must be used for work related matters only.

3.33 Staff email signatures must only be used in matters related to official Oakhill College business.

Mobile Phones and Smart Device Communication Tools - STUDENTS

3.34 Please refer to the Student Diary for Acceptable Use of Mobile Phones and Smart Devices policy and guidelines and ICT Infrastructure Usage.

3.35 Mobile phones or any other devices may be confiscated or searched if a member of staff has reason to believe the device or its use is in breach of this policy and Oakhill College rules and regulations.

4.0 Evaluation and Review

The College Principal is to ensure that this Policy is monitored and reviewed to ensure it is up to date with all legal requirements and legislative changes and reviewed according to the policy review schedule.

5.0 Explanatory Notes and Definitions

Definitions:

ICT Resources	ICT resources includes but is not limited to all networks, systems, software and hardware including local area networks, wide area networks, wireless networks, intranets, College email systems, computer systems, software, servers, desktop computers, printers, scanners, personal computers (desktops, notebooks and tablets), mobile phones, portable storage devices including digital cameras and USB memory sticks, hand held devices and other ICT storage devices.
User/s	Any person using Oakhill College ICT resources.
Infrastructure	ICT infrastructure includes for example Wi-Fi software and hardware, data cables, Access Points, firewalls, ICT software monitoring systems, surveillance software and hardware, localised and cloud servers and related hardware and software

6.0 Supporting Documents

- Information Security Policy
- Mobile and Smart Device Policy
- Privacy Policy
- Records Storage & Retention Policy
- Staff Social Media Policy
- Workplace Surveillance Policy
- Staff Code of Conduct Policy
- Bullying & Harassment policy
- Child Protection Policy
- Work Health and Safety Policy
- NSW Department of Education Communication Devices and Associated Services Policy
- College Diary

7.0 Appendices