STUDENT ICT ACCEPTABLE USE GUIDELINES

Purpose:

To -

- maintain an ethical and amicable learning environment
- ensure that ICT systems in the College are not used improperly or illegally

Relevant to:	All Members of Staff Volunteers
Responsible Officer(s):	Principal ICT Manager
Date of Introduction:	March 2003
Date of Review:	June 2011
Modification History:	December 2008 December 2011 March 2013 July 2015 October 2015
Related Documents:	Appendix II*: ICT Behaviour Support and Consequence Plan* Student Use of Online Services Appendix 1: *Student ICT Acceptable Use Agreement Form* Student MacBook Agreement Personal Electronic Technology Guidelines

BACKGROUND

The Internet and online services provided at Trinity Catholic College are intended for research and learning and communication between students and staff. This document aims:

- To list the rules and acceptable use for ICT (Information and Communication Technology) resources
- To ensure that students of the College use ICT resources in a responsible and ethical way to promote a secure and safe learning environment
- Providing learning experiences that maximise the benefit of the Internet and network services to enrich and enhance classroom practices
- To outline consequences of ICT breaches

Students should be aware that a breach of these guidelines may result in the termination of computer privileges and disciplinary action. This may include referral to the Police.

1. The College

The College Student ICT Acceptable Use Policy applies to all Information and Communication Technology (ICT) devices and services used within the College. This includes but is not limited to:

- Infrastructure, Windows computers, Windows laptops, iMacs, MacBooks, equipment and technologies owned or operated by the College.
- Laptops, mobile phones, iPods, iPads, storage devices and any other ICT device privately owned by students.
- Internet services
- Email
- Cameras, scanners, printers, photocopiers, audiovisual equipment and devices

The staff at Trinity Catholic College will take all reasonable measures to ensure that students use the ICT resources correctly, for educational purposes throughout the College.

2. ICT Technical Support

The College has two technical support centres, the ICT Hub, located in the SMS Library and the ICT Cave located in the 80's block on SJS. There is also an online helpdesk accessible via email to helpdesk@trinitylismore.com or the College Intranet.

3. Parents and Carers

The appropriate use of ICT is the joint responsibility of students, parents/carers and College staff. Therefore, parents and carers should share with the College the responsibility for setting and conveying standards for acceptable use when using electronic media and information sources. It is important for the parent/carer to have read and understand this document.

Students *must* have signed the *Trinity Student ICT Acceptable Use Agreement Form* (*Appendix 1*) to be allowed access to the College's ICT systems and computers.

4.Students

As users of the College's ICT systems and computers, students have important responsibilities when using this technology. By signing the *Trinity Student ICT Acceptable Use Agreement Form* (*Appendix 1*), the student is agreeing to the following conditions outlined below. It is important to realise that the College reserves the right to determine other conditions as appropriate to a particular situation.

4.1. Unlawful and inappropriate use

College ICT resources must not be used to download, display, print, save or send material that others may find offensive, for example pornographic, violent or racist material, obscene language or any material that is contrary to the ethos of the College. In particular, accessing or sending any material or emails in violation of any State, Federal or International regulation is prohibited.

If a student accidentally accesses inappropriate material, they should:

- Not show others
- Turn off the screen or minimize the window
- Report the incident to a teacher immediately.

4.2. Copyright and intellectual property

Computer software must be used in accordance with licence agreements.

Students must not make an unauthorised reproduction of material protected by copyright, or use audio-visual material without permission from the copyright owner. This includes material on the Internet, CDs, DVDs and any other electronic storage device. The legal rights of software producers and network providers, and copyright and license agreements must be honoured. A student who infringes copyright may be personally liable under the law.

These rules also apply to any privately-owned ICT equipment/device a student brings to the College or to a College-related activity. Any images or material on such equipment/devices must be appropriate to the College environment.

Any software, music or videos installed on the College's MacBooks must be legally purchased – specifically, the College reserves the right to remove any "pirated" software, music or videos.

4.3. Cyber Bullying, Peer Pressure, Spam

Students must not engage in harassment, bullying, spamming, illegal behavior, malicious blogging or similar antisocial behaviors. Students who use a social networking or blogging site for antisocial behavior, such as bullying a fellow student, will be subject to the College regulations regarding such behavior. The matter may be referred to the police for further investigation.

4.4. Email, Privacy and Personal Safety

Students must respect others' privacy and academic property.

Each student has a College email address. No other email service apart from the College email is permitted while at the College eg Hotmail, Yahoo. E-mail is provided by the College for educational use, though the College understands that personal e-mails are sometimes received.

Chain letters and other unsolicited email must not be forwarded. Students must not send full school or large group e-mails unless you have the permission of the Assistant Principal, the ICT Manager or your Head of House/Head of Department approves it for educational purposes.

Use of the Internet and email carries the risk of bringing students into contact with individuals who may be unfriendly, rude or exploitative. Students should not reveal personal details about themselves or others.

Email documents are stored and may be used in future legal matters.

4.5. Monitoring and Access to Student Files and Activity

The College may exercise its right to monitor the use of the College's ICT resources to:

- Ensure that the systems and networks are functioning properly
- Protect against unauthorised access
- Ensure compliance with the *Trinity Student ICT Acceptable Use Agreement*

All Internet use is logged and can be checked at any time.

The College reserves the right under "Duty of Care" to access files and email as the ICT Manager deems necessary. The ICT staff have the right to delete any files that are deemed to be inappropriate under the *Trinity Student ICT Acceptable Use Agreement* (eg games, filesharing or "hacking" programs).

College staff have the right to remotely view student's computer screens and remotely manage their use.

4.6. Network Security

Each student will be issued with a computer account which can be used to access the Internet and other online services. Each student is responsible for all activity under their computer account. Access to the College network and Internet must only be made via the student's authorised account and password, **which must not be given to any other person**. It is the student's responsibility to log out of the computer properly at the end of each lesson.

Security problems *must* be brought to the immediate attention of the ICT Manager or ICT
staff. The problem must not be demonstrated to other
students.

Security breaches which are not permitted and have serious consequences include:

- Attempting to gain unauthorised access to any information resources, systems or networks, or interfere with another person's work.
- The use of Peer to Peer networking [Limewire, utorrent, etc and Instant messaging (MSN, iChat, etc)] between students or to others on the Internet.
- The running of programs on the system that have not been sanctioned by the ICT Manager

- The use of anonymous proxies or other techniques to bypass the College’s proxy server (eg to allow access to FaceBook, YouTube, etc)
- Networking other computers together by using cables or wireless networks, or disconnecting or modifying computer or network cables in the computer rooms.
- Playing of networked games (eg Halo, Quake) or the uploading of these games or any other files to unauthorised parts of the College network (eg, the *profiles* directory)
- Deliberately engaging in any activity that may cause damage to the College's ICT resources, or to anyone else's computer equipment. This includes, but is not limited to, the uploading or creating of computer viruses. Hardware and software vandalism will result in the student having to pay all costs to repair damage, including any labour charges.

4.7. Assessments and Backups

Failure of hardware or software will not be deemed as an acceptable reason for late submissions of an Assessment Task.

It is the student’s responsibility to make a backup of their school work and personal files. The ICT staff are not responsible for loss of these files when fixing a computer problem.

Refer to *Assessment Policy* found in Assessment Handbooks

4.8. Printing usage

Students will be charged for all printing in classrooms and libraries at the College. A preset amount of printing credit will be given to students at the start of the year.

Students can pay for more printing credit at the libraries.

4.9. MacBooks (only for students on the MacBook program)

Refer also to Trinity Student MacBook Agreement

4.10. Use of privately owned laptops or mobile devices

Refer also to Trinity Personal Electronic Technology Policy

4.11. Management of Infringements

Students are expected to be aware of the *Student ICT Acceptable Use Guidelines*. Where infringements occur the following **Behaviour Support and Consequence Plan** will serve as a guide to follow up action.

Appendix II

Trinity Catholic College - Student ICT Acceptable Use Guidelines
Behaviour Support and Consequence Plan

This Consequence Plan is divided into 3 Levels:

Level 1- Minor infringement. Issues managed at the classroom level with utilisation of the Time Out process.

Level 2 – Medium infringement or repetition of Level 1 behaviours. Consequences include Subject Time out and ban from the network for 1-2 weeks as well as parental contact.

Level 3(a) – Major infringement or repetition of Level 2 behaviours – First Offence. Consequences include: replacement of damaged equipment, after school detention, 1 day internal/external suspension, expulsion, ban from the network for 20 school days, parental contact, police involvement for infringements involving the Law.

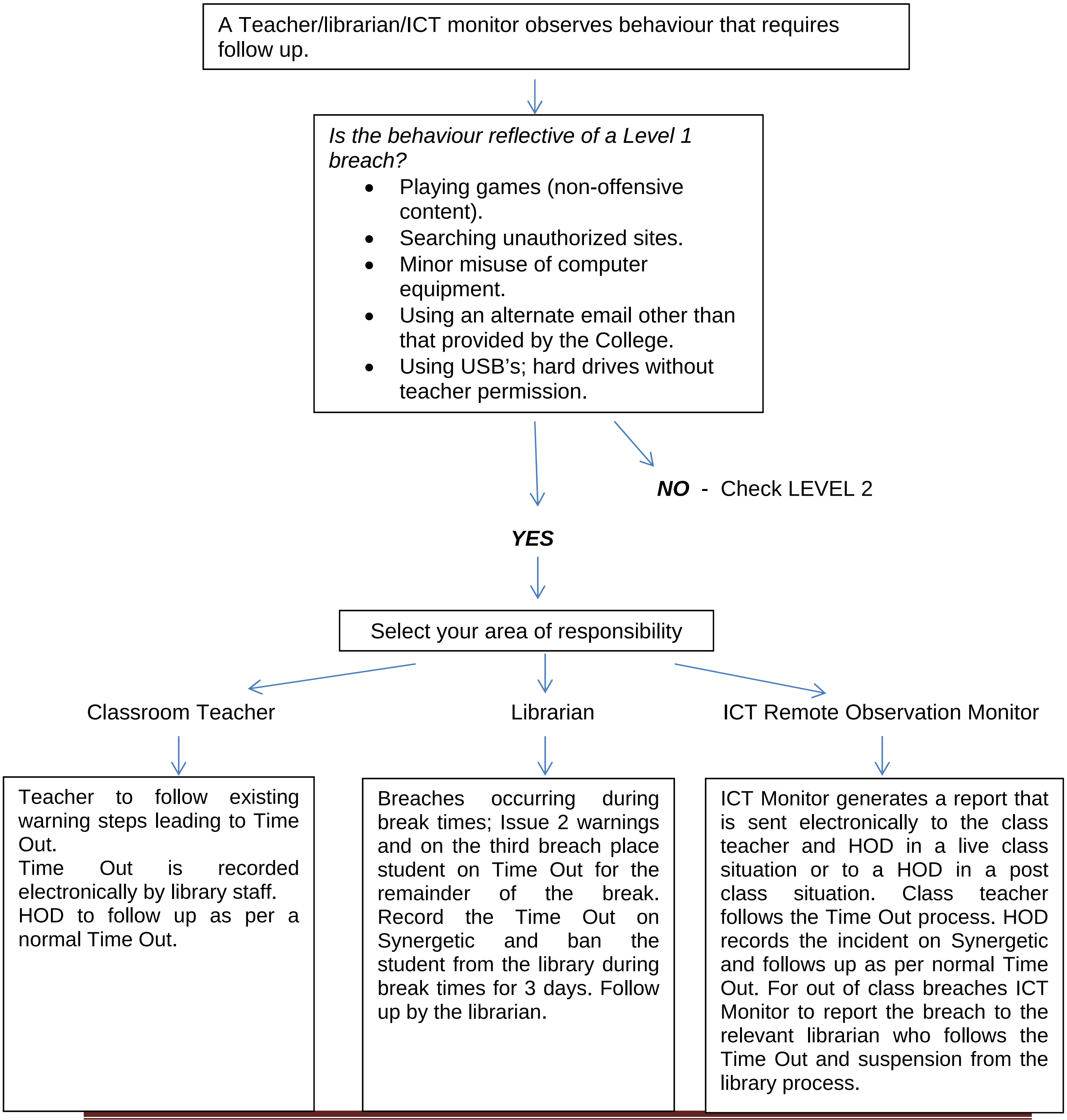
Level 3(b) – Major infringement or repetition of Level 2 behaviours – Second Offence. Consequences include: Extended external suspension, expulsion, network bans for 1 term, Principal/Parent meeting, police involvement for matters relating to the Law.

Appendix III

Trinity Catholic College Lismore Behaviour Support and Consequence Plan

These guidelines ask the teacher to categorise the breach into one of 3 levels and then to follow the recommended course of action.

LEVEL ONE



A Teacher/librarian/ICT monitor observes behaviour that requires follow up.

Is the behaviour reflective of a Level 1 breach?

- Playing games (non-offensive content).
- Searching unauthorized sites.
- Minor misuse of computer equipment.
- Using an alternate email other than that provided by the College.
- Using USB's; hard drives without teacher permission.

NO - Check LEVEL 2

YES

Select your area of responsibility

Classroom Teacher

Teacher to follow existing warning steps leading to Time Out.
Time Out is recorded electronically by library staff.
HOD to follow up as per a normal Time Out.

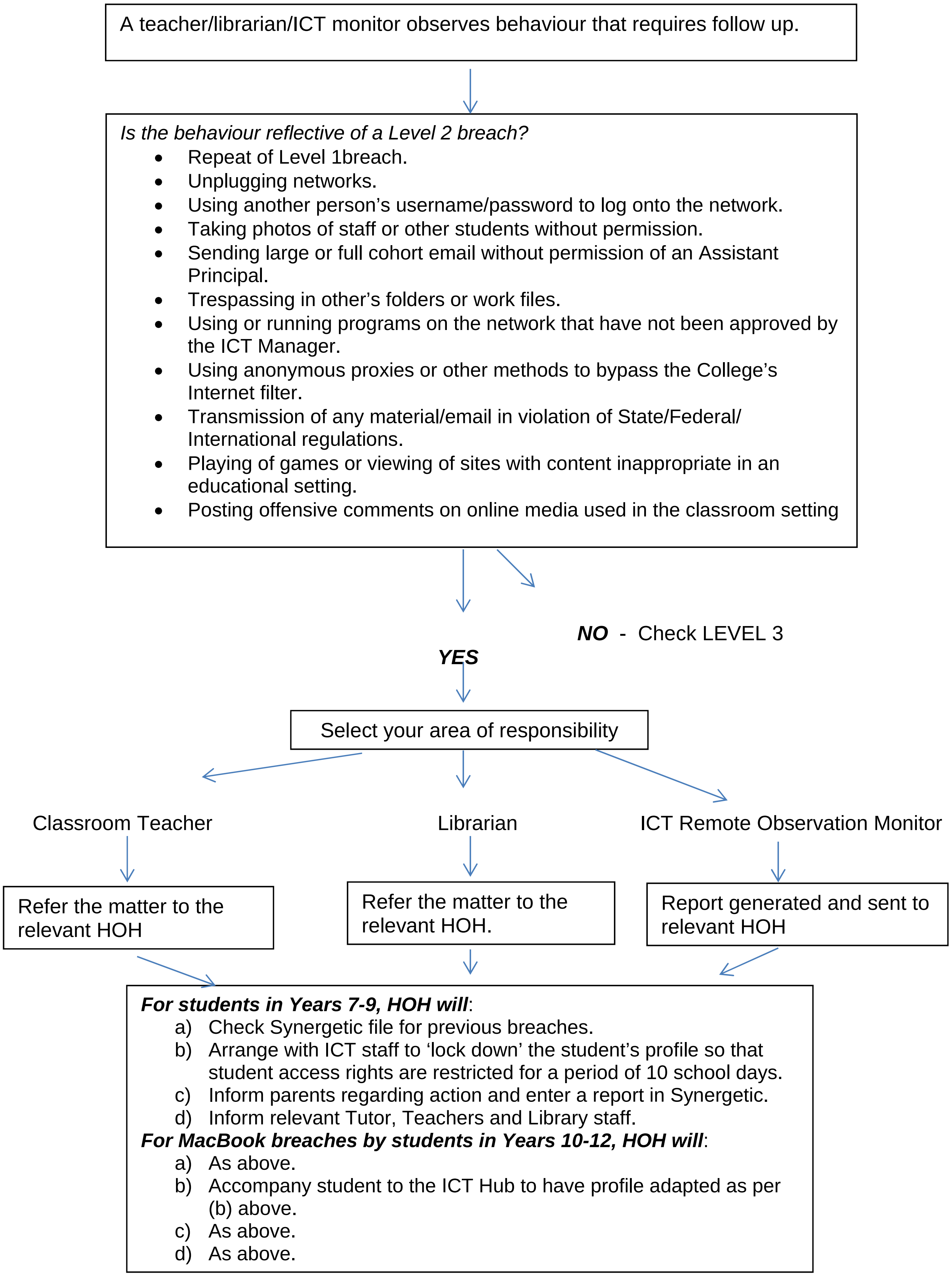
Librarian

Breaches occurring during break times; Issue 2 warnings and on the third breach place student on Time Out for the remainder of the break. Record the Time Out on Synergetic and ban the student from the library during break times for 3 days. Follow up by the librarian.

ICT Remote Observation Monitor

ICT Monitor generates a report that is sent electronically to the class teacher and HOD in a live class situation or to a HOD in a post class situation. Class teacher follows the Time Out process. HOD records the incident on Synergetic and follows up as per normal Time Out. For out of class breaches ICT Monitor to report the breach to the relevant librarian who follows the Time Out and suspension from the library process.

LEVEL TWO



A teacher/librarian/ICT monitor observes behaviour that requires follow up.

Is the behaviour reflective of a Level 2 breach?

- Repeat of Level 1breach.
- Unplugging networks.
- Using another person’s username/password to log onto the network.
- Taking photos of staff or other students without permission.
- Sending large or full cohort email without permission of an Assistant Principal.
- Trespassing in other’s folders or work files.
- Using or running programs on the network that have not been approved by the ICT Manager.
- Using anonymous proxies or other methods to bypass the College’s Internet filter.
- Transmission of any material/email in violation of State/Federal/ International regulations.
- Playing of games or viewing of sites with content inappropriate in an educational setting.
- Posting offensive comments on online media used in the classroom setting

NO - Check LEVEL 3

YES

Select your area of responsibility

Classroom Teacher

Librarian

ICT Remote Observation Monitor

Refer the matter to the relevant HOH

Refer the matter to the relevant HOH.

Report generated and sent to relevant HOH

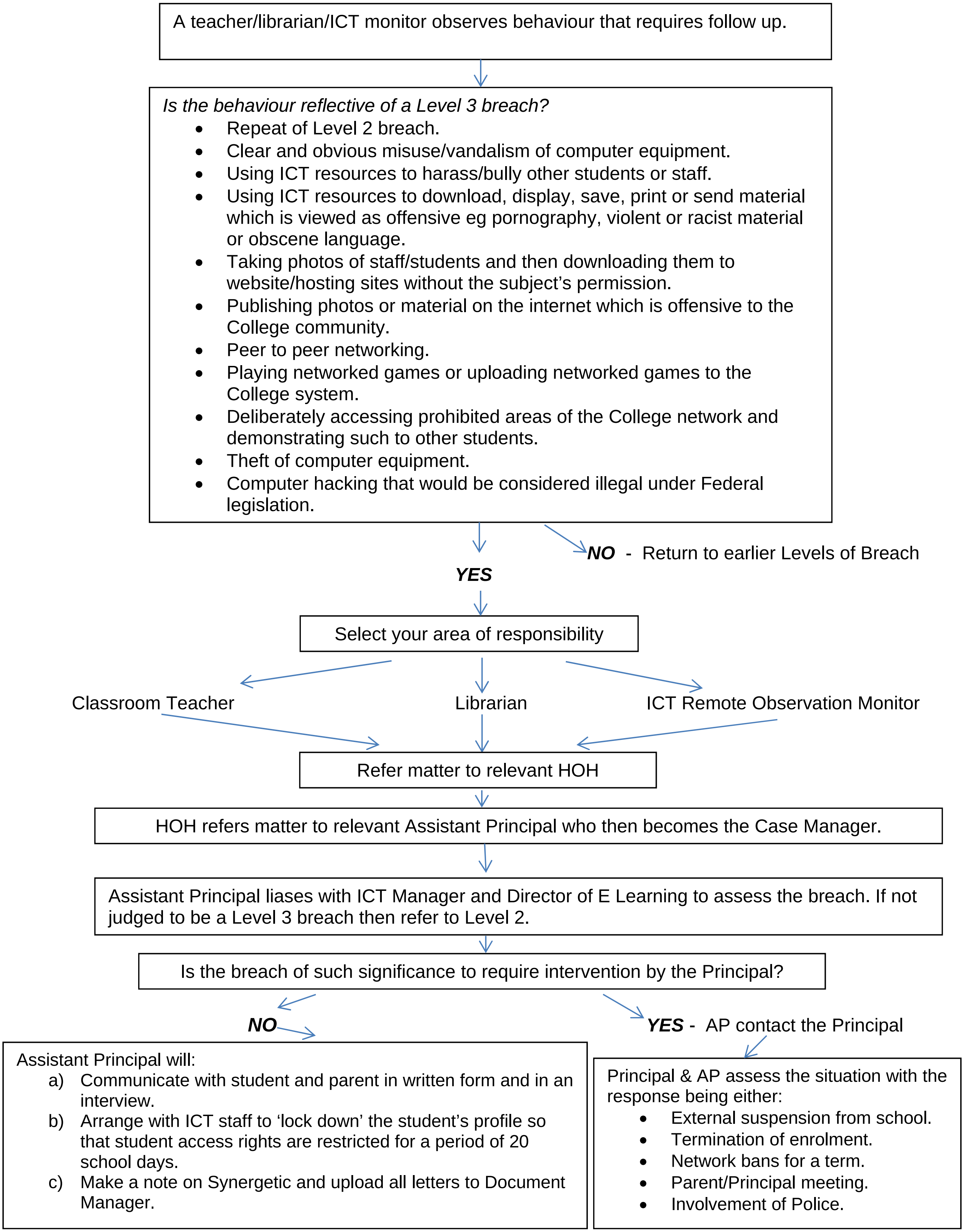
For students in Years 7-9, HOH will:

a) Check Synergetic file for previous breaches.
b) Arrange with ICT staff to ‘lock down’ the student’s profile so that student access rights are restricted for a period of 10 school days.
c) Inform parents regarding action and enter a report in Synergetic.
d) Inform relevant Tutor, Teachers and Library staff.

For MacBook breaches by students in Years 10-12, HOH will:

a) As above.
b) Accompany student to the ICT Hub to have profile adapted as per (b) above.
c) As above.
d) As above.

LEVEL THREE



A teacher/librarian/ICT monitor observes behaviour that requires follow up.

Is the behaviour reflective of a Level 3 breach?

- Repeat of Level 2 breach.
- Clear and obvious misuse/vandalism of computer equipment.
- Using ICT resources to harass/bully other students or staff.
- Using ICT resources to download, display, save, print or send material which is viewed as offensive eg pornography, violent or racist material or obscene language.
- Taking photos of staff/students and then downloading them to website/hosting sites without the subject's permission.
- Publishing photos or material on the internet which is offensive to the College community.
- Peer to peer networking.
- Playing networked games or uploading networked games to the College system.
- Deliberately accessing prohibited areas of the College network and demonstrating such to other students.
- Theft of computer equipment.
- Computer hacking that would be considered illegal under Federal legislation.

NO - Return to earlier Levels of Breach

YES

Select your area of responsibility

Classroom Teacher

Librarian

ICT Remote Observation Monitor

Refer matter to relevant HOH

HOH refers matter to relevant Assistant Principal who then becomes the Case Manager.

Assistant Principal liases with ICT Manager and Director of E Learning to assess the breach. If not judged to be a Level 3 breach then refer to Level 2.

Is the breach of such significance to require intervention by the Principal?

NO

Assistant Principal will:

a) Communicate with student and parent in written form and in an interview.
b) Arrange with ICT staff to 'lock down' the student's profile so that student access rights are restricted for a period of 20 school days.
c) Make a note on Synergetic and upload all letters to Document Manager.

YES - AP contact the Principal

Principal & AP assess the situation with the response being either:

- External suspension from school.
- Termination of enrolment.
- Network bans for a term.
- Parent/Principal meeting.
- Involvement of Police.

Appendix I

Student ICT Acceptable Use Agreement Form

Student Name:
____

Year Group ***(please circle):*** **7 8 9 10 11 12**

Student Declaration

I have read and understood the Student Acceptable Use Agreement. I agree to abide by the guidelines. I accept that the College reserves the right to suspend students from the use of the computer facilities for breaching this Agreement, and that further disciplinary action may be taken for serious and/or repeated breaches.

I accept that College ICT staff can remotely view and control College computers and that I am responsible for backing up my computer files on a regular basis.

Student Name: ....**Date**: …../…../…..

Student Signature: ……………………………………………