

John Paul College Policy

CYBERSAFETY

RATIONALE

This policy is designed to meet the school statutory obligations to maintain a safe learning environment. The overall goal is to maximise the education benefits of digital technologies while minimising the risks. The maintenance of the physical and emotional safety of the learning environment is of paramount concern in accordance with the Catholic character of John Paul College and the high moral standards expected of both staff and students. The policy applies to all employees of the Board (i.e. teaching, support and ancillary staff) and all students. It also applies to teacher and other professional trainees assigned to the school from time to time.

PURPOSE

1. To ensure use of the Internet and other digital technologies at John Paul College is limited to educational and personal usage appropriate to the school environment. Other technologies include mobile phones (including Smart Phones), I-Pods, Tablets such as I-Pads and other technologies associated with Internet use e.g. web cam and other technology involving still and video photography. Included, too, are similar technologies still being developed.
2. To ensure that the digital technologies at John Paul college are available to staff and students under specific conditions, as outlined in their signed Use Agreements. (Appendices 1, 2, 3 and 4)
3. To provide appropriate training for staff using these technologies and make provision for appropriate professional development needs.
4. To establish and enforce appropriate Cybersafety measures to ensure the safety of the school learning environment and to ensure action is taken if these safety regulations are breached by students or staff.
5. To ensure that where technologies are used in places other than specialised rooms, specific cybersaftey protocols are established, documented and publicised appropriately (see Departmental and Classroom Cybersafety 5.19.1)
6. To develop the establishment and maintenance of a Cybersafety programme through the auspices of the E-Learning Committee and E-learning Coordinator.
7. To ensure regular reporting to the Board of Trustees of the management of the Cybersafety programme.
8. To ensure that breaches of Cybersafety policies and regulations are investigated and if appropriate disciplinary action is taken.

GUIDELINES

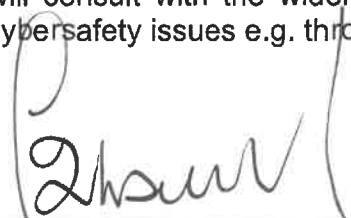
1. The E-Learning Committee, comprising the E-Learning Coordinator, the Network Manager and a representative from each faculty (see E-Learning 1.12) is charged with advising the Principal on the establishment and maintenance of the school “cybersafety programme”. This Cybersafety programme will include three components:
 - a) An infrastructure of appropriate policies, procedure and use agreements
 - b) An effective electronic security system, and
 - c) A comprehensive Cybersafety education programme for the school community.

The E-Learning coordinator will be the main point of contact for all issues of incidents involving communication technologies in the school, and will report to the Principal.

2. On enrolment, all students must read and sign the ‘John Paul College Intranet and E-Learning Resources Acceptable Use Agreement (Appendix 1) and a Digital Citizenship Contract (Appendix 2). These agreements outline the regulations and conditions under which computers and communication technologies may be used at school to ensure the safety of the school learning environment.
3. The Acceptable Use Agreement (Appendix 1) must also be signed by a parent/caregiver and is to be handed in to the office where it will be filed for the record.
4. Where a student wished to bring their own personal electronic device parents/caregivers are to sign a ‘Bring Your Own Device Agreement’ (Appendix 3). Such devices include Smart Phones, Tablets e.g. I-Pads. Laptops, Netbooks and I-Pods and their equivalents.
5. Those students who do not have signed Use Agreements on file will not be permitted to access the relevant school technologies; their parents/caregivers will be informed of the situation.
6. At the commencement of their employment, all Board Employees) teachers, support and ancillary staff, including the caretaker, groundsmen and such personnel as Teacher Trainees and Relief Teachers) must sign the ‘Staff Intranet and E Learning Resources Use Agreement’ (Appendix 4).
7. For staff working with students, the Agreement includes details of their responsibilities to actively supervise/monitor student Internet use. The degree and type of that supervision may vary, dependent on the type of technology concerned, the physical location of the equipment and whether or not the activity is occurring in the classroom.
8. The agreement also informs staff of the limits to their own use of the Internet within the school environment, and of privacy issues associated with confidential information on the school network. Educational material on Cybersafety will be provided by the E-Learning Committee to staff and students and to parents/caregivers e.g. posters and information in school homework diaries. Additional education will be delivered where relevant, through teaching programmes.
9. Basic training for staff in Cybersafety issues and procedures will be addressed by the E-Learning Committee, as will professional development requirements. There will be a special focus on the skills/training of the Network Manager. Other specific areas which may need to be addressed include the management of the school’s website.

10. The necessary procedures will be put into place by the school to address Cybersafety issues in all venues where the Internet and other communication technologies are accessed by staff or students.
11. The school will provide an effective electronic storage system which is safe and financially practicable. The school will continue to refine methods to improve Cybersafety.
12. Any breaches of Cybersafety regulations (by staff or students) should be reported to the E-Learning Coordinator. This includes misconduct facilitated by the use of communication technologies e.g. harassment. Less serious matters should be documented and reported to the Coordinator at a convenient time.
13. If the matter appears to be serious, that report should be made immediately. If the Coordinator is not available, the report should be made to another member of the Senior Leadership Team or directly to the Principal. The matter will then be dealt with according to the school's usual disciplinary procedures (including the need to provide counselling and support) with a special focus on Cybersafety issues.
14. The Board supports the right of the school to check communication technology related work or data by staff or students at any time in line with the Privacy Act and the JPC Search and Surrender policy, and to carry out a comprehensive investigation of any breaches of the school's Cybersafety policies. Such breaches will be taken seriously and be dealt with through the school's disciplinary and support systems. If illegal material or activities are suspected, the matter will be reported to the Police or the Department of Internal Affairs Censorship Committee.
15. The school will consult with the wider school community and provide opportunities to learn about Cybersafety issues e.g. through parent information evenings.

Ratified by Board



Signed by B.O.T. Chair

27.06.2010

Date

Next review

Signed by B.O.T. Chair

Date 2019

APPENDICES

Appendix 1: John Paul College Intranet and eLearning Resources Acceptable Use Agreement for Students
(Signed by Parents/Caregivers and Students)

Appendix 2: Digital Citizenship Contract
(Signed by Students)

Appendix 3: Bring Your Own Devices Agreement
(Signed by Parents/Caregivers)

Appendix 4: Staff Intranet and E Learning Resources Use Agreement
(Signed by all teachers and staff)