PRESENTATION COLLEGE, BRAY

INFORMATION AND COMMUNICATIONS TECHNOLOGY, ACCEPTABLE USE POLICY FOR THE WHOLE SCHOOL COMMUNITY.

THIS POLICY WAS RATIFIED BY THE BOARD OF MANAGEMENT OF THE COLLEGE ON JUNE 3RD 2011 AFTER CONSULTATION WITH ALL STAKEHOLDERS.

THIS POLICY WILL BE SUBJECT TO REGULAR REVIEW AS TECHNOLOGIES AND USES CHANGE AND EVOLVE.

Presentation College is a Catholic Boys' School under the auspices of the Presentation Brothers Schools Trust.   The staff, students and parents of Presentation College, Bray, seek to promote a safe, caring environment and a well-balanced student-centred curriculum which encourages self-reliance, respect and responsibility.

Parents are recognised as the primary educators while teachers nurture and develop student learning. In partnership, we hope to enable all students to leave school with the skills necessary to participate fully in society and to live independent and fulfilled lives.

P.B.S.T

> **"All are welcome, all are included, all are enriched"**

ACCEPTABLE USE POLICY
PRESENTATION COLLEGE, BRAY
INFORMATION AND COMMUNICATIONS
TECHNOLOGY RESOURCES IN THE COLLEGE

The school's information and communications technology resources, including email, Internet access (World Wide Web) and Intranet are provided for educational purposes. These resources are provided as an educational tool the purpose of which is to enhance teaching and learning. The Board of Management has prioritised provision of the most up to date ICT resources and fully recognises the value of ICT to the college community. While the safety of each member of the school community is a prime concern, the Board is also concerned for the good reputation of the College. The consequences for any action which might damage the reputation of the College or lead to legal actions or claims against the College will rest with the perpetrator of said actions. Access by students to ICT resources is allowed only under the direct supervision or direction of a teacher. Filtering software will be used in order to minimise the risk of exposure to inappropriate material. The College will regularly monitor Internet access. Virus protection will be installed and regularly updated. Adherence to the following policy is necessary for continued access to the school's technological resources.

Users must
1. Respect and protect the privacy of themselves and others.
    o Use only assigned accounts. Passwords must be protected. Any use of ICT under a password will be the responsibility of the person to whom the password was assigned.
    o Not view, use, or copy passwords, data, or access networks to which they are not authorised. Use of privately owned devices to access College networks is strictly prohibited.
    o Not distribute private information about others or themselves.
    o Not have access to chat rooms or other electronic communication without school approval and in the case of students, teacher supervision.
2. Respect and protect the integrity, availability, and security of all electronic resources.
    o Observe all network security practices. The use of personal data storage devices, eg. flash drives, is strictly prohibited.
    o Report security risks or violations to a teacher, tutor, year-head or management.
    o Not destroy or damage data, networks, or other resources that do not belong to them, without clear permission of the owner.
    o Not download or install any software, shareware and freeware.

- o Not create or willfully disseminate computer viruses. Be sensitive to the ease of spreading viruses and take steps to ensure that discs and files are virus free.
- o Not alter, view or change computer settings or system configurations.
3. Respect and protect the intellectual property of others.
    - o Not infringe copyrights (no making illegal copies of music, games, films etc).
    - o Not plagiarise.
4. Respect and practice the principles of community.
    - o Communicate only in ways that are kind and respectful. Cyber bullying is a very serious issue. Users must refrain from any form of communication which could constitute bullying.
    - o Not access social networking sites.
    - o Report threatening or discomforting materials to a teacher.
    - o Not intentionally access, transmit, copy, or create material that violates the school's code of conduct (such as messages that are pornographic, threatening, rude, discriminatory or meant to harass).
    - o Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
    - o Not use the resources to further other acts that are criminal or violate the school's code of conduct.
    - o Not send spam, chain letters, or other mass unsolicited mailings.
    - o Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

Consequences for Violation. Violations of these rules may result in disciplinary action, including verbal warnings, contact with parents/guardians of students, loss of a student's privileges to use the school's information technology resources and in extreme cases suspension or expulsion.
Supervision and Monitoring. School and network administrators and their authorised employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. College authorities reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

PARENTS, PLEASE DISCUSS THESE RULES WITH YOUR SON TO ENSURE HE UNDERSTANDS THEM.
THESE RULES MAY ALSO PROVIDE A GOOD FRAMEWORK FOR YOUR SON'S USE OF COMPUTERS AT HOME, AT LIBRARIES, OR ANYWHERE.
FOR MORE INFORMATION, SEE www.cybercrime.gov.