St Brigid's College
Horsham

INFORMATION COMMUNICATION AND TECHNOLOGY (ICT) POLICY

1. ABOUT THIS POLICY

This policy:

- describes the requirements and guidelines which all people who have access to the School's electronic mail (**'email'**) system and/or Internet/Intranet must comply with;
- describes the requirements in relation to the use of school-owned computers, tablets, and all other forms of Information Communication and Technology resources (**"ICT resources"**) applications and devices;
- describes the requirements in relation to the use of electronic devices not owned by St Brigid's College;
- applies to all staff who use or have access to the School's ICT resources (including, but not limited to employees, emergency teachers and student teachers) (**"Computer Users"**);
- Applies to all students who use or have access to the School's ICT resources; and
- is to be read in conjunction with the related Policies listed at the bottom of this Policy.

2. POLICY

Computers, computer systems, email and Internet/Intranet facilities all form part of the school's ICT resources, and are the School's property even where access is gained from a personal or home computer or other electronic device.

The School allows access to, and the use of email and/or the Internet, for legitimate work and education related purposes. This policy contains the School's requirements regarding the use of these systems.

3. ACCESS TO THE SCHOOL'S EMAIL SYSTEM

Access to the School's computer resources (such as email and Internet) is a privilege not a right.
No one is permitted to access the School's email system, without:

- reading and understanding this policy;
- authorisation from the School and an individual password from the School's Network Administrator.

If the School considers that a Computer User has in any way failed to comply with this policy, it may:

- immediately remove the Computer User's access to any part of the School's computer system (including email or Internet); and/or
- take disciplinary measures against the Computer User (which may include summary dismissal for a staff member or expulsion for a student).

4. APPROPRIATE USE OF THE EMAIL SYSTEM

Email must only be used for work/education related communications and must not be used inappropriately.

Computer Users that are staff members must ensure that all external correspondence by email is identified as coming from the School and contains the following disclaimer:

> *"IMPORTANT! This email and any attachments may be confidential. If received in error, please contact us and delete all copies. St Brigid's College does not represent or warrant that the attached files are free from computer viruses or other defects. The attached files are provided, and may only be used, on the basis that the user assumes all responsibility for any loss, damage or consequence resulting directly or indirectly from the use of the attached files, whether caused by the negligence of the sender or not. The liability of St Brigid's College is limited in any event to either the resupply of the attached files or the cost of having the attached files resupplied. Any representations or opinions expressed in this email are those of the individual sender, and not necessarily those of St Brigid's College*

All people using the School's email system must <u>not</u> use it in any of the following ways:

- in a way that may be considered offensive, defamatory, obscene, pornographic, discriminatory, insulting or disruptive to any other person (for example, pictures of naked people, semi clothed people, personal comments about colleagues, students or the School's administrators);

- to access, view, download, print or send messages or attachments (including to your home email address), which include:
  - language that is not appropriate in the workplace (such as swearing or sexually explicit references);
  - sexually explicit message or pictures;
  - offensive or inappropriate cartoons or jokes;
  - unwelcome propositions or love letters;
  - ethnic or racial slurs; or
  - any material which contains disrespectful comments about people with disabilities, or people's sexual orientation, or any person's physical attributes;

- to access other people's email accounts;

- to join a mailing list or chat group, post messages to news groups, or engaging in on-line purchasing or selling unless instructed by authorized personnel of the school to do so;

- for sending chain mail, gambling, participating in on-line games, retrieving games or screen savers;

- to distribute the copyright material of third parties, including software, database files, documentation, pictures, articles, graphic files, text or other downloaded information;

- for intentional dissemination of any computer viruses;

- for personal advertising or for financial or commercial gain;

- for disclosing or distributing the School's confidential information;

- for responding to external requests for information or complaints through email unless it is the computer User's specific responsibility to do so;

- for sending, forwarding, printing or receiving any material or data which does not comply with the School's policies and procedures, or which is contrary to the School's best interests; and

- collect, store, or disseminate personal information (information or an opinion that can identify a person) or sensitive information (personal information or an opinion about an individual's: racial or ethnic origin; political opinions, membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; criminal record, or health information about an individual) while using the School's computer resources, unless the Computer User has the prior consent of the person concerned.

The School understands that Computer Users cannot always control the messages that are sent to them. However, Computer Users must discourage third parties (such as family, friends, other students or workmates) from sending inappropriate messages to them.

If a Computer User receives an inappropriate message or attachment to an email he or she must:

1. Send an email to the person who sent the inappropriate email which indicates that such messages should not be sent. An appropriate form of words is:

   "Please do not send me this type of material again. The contents of this email do not comply with the School's electronic mail policy. In sending me this email you are breaching the School's policies and putting me at risk of doing so. A breach of the electronic mail policy has serious consequences."

2. You may wish to forward a copy of this response (together with the inappropriate email) to the School's Computer Network Administrator.

3. Delete the email.

5. APPROPRIATE USE OF THE INTERNET/INTRANET SYSTEM

The School's Internet access facilities must only be used for authorised work or education related purposes. The School's Internet facilities must not be used to:

- Access, view, download, print, disseminate or post any material that may be considered inappropriate, offensive, defamatory, obscene, pornographic or discriminatory including material that is sexually explicit or that has racist, sexist, political or religious content or which includes inappropriate comments in relation to sexual orientation, disabilities or any other physical attributes;

- Attempt to probe or "hack" security mechanisms at the School or any other Internet sites;

- Post any information on Internet news groups, bulletin boards or any other social media forums on behalf of the School unless specifically authorised to do so; or

- Download/copy information from articles on the Internet – unless the Computer User has adhered to the same protocols for recognising source information that apply to the use of hard copy documents as reference or research material.

While using the School's Internet facilities, Computer Users **must**:

- Check that any files downloaded are virus free before they get into the School network.
- If downloading files from the internet:

    1. Download files to a computer hard disc/USB so that they can be virus checked prior to use;
    2. Arrange with the School's Computer Network Administrator to immediately install an up-to-date virus checker if there is not an up-to-date virus checker on the Internet connected computer; and
    3. Only transfer internet files into the School's network system once these internet files are proven to be free of viruses.

While using the School's Internet facilities, Computer Users **must not**:

- Misrepresent or attempt to misrepresent their identity; or
- Subscribe to Internet or mail lists without specific authorisation from the School; or
- Download files directly from the internet into the School's network system without complying with the requirements set out above.

6. APPROPRIATE USE OF SCHOOL-OWNED ICT RESOURCES

1. Computer users who are teachers will incorporate the use of ICT into their pedagogy on a regular basis, and acknowledge this will involve more than accessing and using SIMON and internet research.

2. All Computer users will;
    a. undertake to use all equipment correctly and ensure that no damage occurs (this includes creation, introduction, or spreading of viruses, physically abusing hardware, altering software settings, introducing foreign software, etc.).

    b. not use another person's password to access either the school network or the Internet.

    c. not disclose or pass on to another any access login, password, code or device (including the printer fob) to anyone, especially from a teacher to a student.

3. Computer users who are staff members, acknowledge that the contents of their home directory, Web browsing history and other electronic information gained or developed whilst performing their duties as a staff member of St Brigid's College, becomes the intellectual property of the school, and must be available to the school when required and must be retained by the school when a staff member leaves the employment of the school.

7. PERSONAL USE OF THE SCHOOL'S ICT RESOURCES

Limited and occasional personal use of the School's email and Internet system is acceptable. However, use of Internet and email must not interfere with the Computers User's work, study or general schooling obligations.

Any use of the School's ICT Resources (including Internet or email) by the Computer User must comply with the terms of this policy. Any breach of the policy while using email or Internet for personal use or legitimate work or education related purposes will result in disciplinary action being taken. Such action may include termination of employment (for staff) or expulsion (for students) and may also necessitate reporting to the appropriate authorities.

8. MONITORING and UPDATING ELECTRONIC DEVICES AND APPLICATIONS

Access to the School's ICT resources (including but not limited to electronic devices, email, Internet facilities, etc.) can and will be monitored by the school.

All electronic device users should be aware that:

- St Brigid's College uses deployment software to 'push out' new and upgraded software applications and to provide remote services to staff and students with their electronic devices and associated software.
- School-provided software will require maintenance and upgrading from time-to-time and as such, remote access to a staff/student device, from ICT staff, may be required without notice.
- The content of both work/study related and personal email and Internet communications may be monitored by the School to ensure compliance with this ICT Policy and with other relevant policies, and to support operational maintenance, auditing and security activities.
- All documents, emails and associated attachments stored on the School's computer system are the School's property and may be viewed by the School; and
- All email and Internet transactions and communications may be monitored and can be intercepted by other parties (including parties other than the School).

9. RESPONSIBILITIES

All Computer Users are personally responsible for complying with this policy.

All Staff are personally responsible for ensuring that employees and students under their supervision are;

- aware of and understand this policy; and
- comply with this policy.

10. LEGAL REFERENCES

Federal and relevant State laws bind the School and its employees. A breach of this policy may result in the School and/or its employees breaching any one of the following pieces of legislation:

Racial Discrimination Act 1975 (Cth);
Disability Discrimination Act 1992 (Cth);
Privacy Act 1988 (Cth)
Education and Training Reform Act 2006
Sex Discrimination Act 1984 (Cth);
Equal Opportunity Act 1995 (Vic)
Child Safe Standards (Ministerial Order 870)

Note: This is not an exhaustive list of the relevant legislation.

11. RELATED POLICIES

Workplace "No Bullying" Policy
Teaching & Learning Policy
Child Safety Policy and Child Safe Code of Conduct
Social Media Policy for Employees
Intellectual Property Policy
Computer Internet & Email Acceptable Use Policy

12. DOCUMENT REVIEW

Prepared: Jan 2010	**Date**	**Comment**
Updated:	**Oct 2016**	**Combining former policies**
Updated:	**Apr 2017**	**Layout updated**
Updated:	**Oct 2019**	**Clause 8 updated**
Due for Review:	**March 2021**	