St Agnes Catholic Primary School

Guidelines for Acceptable Use of Technology

This Acceptable Use of Computer and Internet Resource Consent Form must be signed and returned prior to students being full access to iPads and other technology resources.

Parent/Guardians Responsibilities: Parents/ Guardians are asked to review and discuss the contents of the *Acceptable Use of Technology Resources* with the student and answer any questions that they may have. Any queries in relation to this material should be directed to *Liam Beatty APRE.*

Student Responsibilities: Students are agreeing to comply with all requirements as set out in the Acceptable Use of Technology Resources policy and all other relevant laws and restrictions in their access to various technology resources through St Agnes and Brisbane Catholic Education Networks.

Guidelines for Acceptable Use of Technology – St Agnes Primary School

This document has been developed to inform users of their rights, responsibilities and obligations when using Computer and Internet resources, consistent with Brisbane Catholic Education's requirements that all such resources are used in an ethical, legal and responsible manner.

The requirements and rules set out below apply to all St Agnes Primary School technology resources whether they are accessed through computers owned by the school or through privately owned devices (for example, accessing school internet through a personal device or telephone).

Please read this document carefully. Each student and his/her Parent/Legal Guardian must sign the acknowledgment to confirm that they understand the requirements of acceptable use and the potential consequences of a breach of this policy.

Responsibilities of Users

1. Students must comply with the rules for accessing technology resources in this document.

Permitted use of technology resources

2. Students must only access **St Agnes Primary School** technology resources for schoolwork. **Students must not:**
    - buy items, applications or services over the internet
    - access or use social media applications or websites
    - access, post or send inappropriate internet or email content
    - amend documents created by another person without that student's consent
    - download, install or use unauthorised applications
    - gain unauthorised access to any system by any means
    - use technology to access documents or content intended for another student

Confidentiality and cybersafety

3. Students should not display personal information about themselves or others in a way which is public. For example, students should not post their own or anyone else's, photos, videos, addresses,

telephone number or other personal details on the Internet or communicate these details in emails. Students should not distribute someone else's personal information without their permission.

4. Where disclosure of personal information is made through authorised avenues (e.g. by the use of email or an official website), users should be aware that invasions of privacy may sometimes occur and it is outside St Agnes' control to prevent such instances from occurring.

5. As per our Cybersafety workshops, students should be aware that persons on the Internet might not be who they say they are. Students must not arrange to meet persons who they have met on the Internet.

6. The operation and maintenance of technology resources often requires the backup of data, the logging of activity and the monitoring of general usage patterns. St Agnes School may also be required to inspect or provide copies of electronic communications where required to by law, or where the investigation of possible misuses of technology resources is required.

Cyberbullying and defamation

7. Students must not use email or the Internet to say mean, rude or unkind things about other people or send threatening, harassing or offensive messages. Improper use of technology resources could amount to defamation.

Security

8. Students must select a secure password and keep their username and password information private. The password should be changed regularly and should be difficult for other people to guess. It is the student's responsibility to log-off their device when directed.

9. Students must not use another person's name and password to access resources.

10. Students must report a suspected breach of security to a teacher.

11. *Copyright* - Just because something is on the Internet it is not freely available - copying or downloading material from the Internet may be a breach of copyright or other intellectual property rights. Students must not use St Agnes technology resources to copy, download, store or transmit any such material that may include music files, movies, videos or any other form of media.

<u>Consequences following a breach of this policy</u>

12. Any breach of this policy will be taken seriously and followed up by a member of the school's Leadership Team.
13. Any known breaches of these Acceptable Use conditions must be reported by St Agnes to Brisbane Catholic Education.
14. Examples of possible consequences range from loss or restriction of access to technology resources, to formal disciplinary action for breach of the School Discipline policy. Students and Parents/Legal Guardians may be financially liable for damage caused to resources.

15. Cases of serious, deliberate, and/or criminal breach may be referred to external authorities.