Gilmore
COLLEGE

INFORMATION TECHNOLOGY USAGE POLICY

Internet Safety and Appropriate Use

Students **must not** deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or discussion intended to provoke a sexual response
- Violence
- Information about committing any illegal activities
- Information about making or using weapons, booby traps, dangerous practical jokes or "revenge" activities
- Chat or social networks (Instagram, Twitter, Facebook) unless directed by a teacher
- Or any site deemed objectionable by a staff member

Students must not:

- Use material from other web sites unless they have permission from the person who created the material. If unsure, they should check with their teacher
- Bring or download unauthorised programs, including games, to the school or run them on school computers. **Online internet games are banned.**
- Delete, add or alter any configuration files or network settings.
- Break software copyright. Copyright is to be observed at all times. It is illegal to copy or distribute school software. Illegal software from other sources is not to be copied to or installed on school equipment.
- Deliberately introduce any virus or programs that reduce system security or effectiveness.
- Attempt to log into the network with any user name or password that is not their own, or change any other person's password.
- Reveal their network password to anyone except the system administrator. Students are responsible for everything done using their accounts. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause school rules to be broken.
- Use or possess any program designed to reduce network security.
- Enter any other person's file directory or do anything whatsoever to any other person's files.
- Attempt to alter any person's access rights; or
- Store the following types of files in their home directory, without permission from their teacher:

  - Program files
  - Compressed files
  - Picture, music or video files, unless they are required by a subject
  - Obscene material – pictures or text
  - Obscene filenames
  - Insulting material
  - Password-protected files
  - Copyright material.

Students must:

- Make frequent back-ups of their work and assignments using a thumb-drive or any other approved storage device. Staff will not accept data loss as an excuse for not handing in work on time.
- Minimise printing at all times by print-previewing, editing on screen rather than on printouts and spell-checking before printing.
- Follow instructions and not access sites or activities that do not have anything to do with the lesson.

Sanctions

Sanctions for violations of this policy may include, but not be limited to, detention, temporary or permanent withdrawal of the student from the Network and for major breaches suspension.

Note: Staff have the right to monitor student's usage of the internet, monitor their IT usage, regularly check their home drives, remove unnecessary files and report any breaches of this policy.

Document Control:

Owner:	Associate Principal	**Implementation and Review:** The Associate Principal is responsible to the College Executive for the continuous monitoring and review of the Information Technology Usage Policy.
Created:	16/10/2013	
Modified:	26/05/2022	
Approved:	26/05/2022	
Next Review:	May 2024	
Policy Location:	S:\AdminShared\Administration Staff\100Administration\109Policy\GILMORE POLICIES	