ALICE MILLER STUDENT INTERNET POLICY

1. The School's Internet Network is for education, not for personal use such as entertainment. Use of the network is a privilege, not a right.

2. Email is not private. The system operators have access to all user account directories and data, email, personal web pages, and any other files stored on system servers.

3. System operators may delete files at any time for storage reasons.

4. Students given log-on access are responsible at all times for the proper use of the computers.

5. Any inappropriate use will result in the cancelling of the privilege of use and other disciplinary action.

6. Network users should change their passwords frequently.

7. Network users shall not give their password information to anyone else, nor allow anyone else to use their account.

8. Students may only get accounts on the network from a teacher at the school.

The following may result in loss of access, contact initiated by the school with parents (where breaches of this policy are committed by students), police involvement, or any other action that the school considers appropriate, and apply equally to staff, students or other people associated with the school:

- Using the network to hack into any other computer system, or to go beyond the user's authorised access on the school network. This includes attempting to login through another person's account, attempting to access another person's file, attempting to disrupt any computer system's performance, attempting to destroy data on any computer system.

- Using the network for commercial purposes, financial gain, advertisements, business endorsements, or religious or political lobbying.

- Using the network to get an email account or web page opening privileges on another service provider.

The following may result in the school's taking disciplinary measures regardless of whether the actions described involve school computers or other devices, or private computers or other devices, and whether the activities take place during school hours or outside school hours, and whether the activities take place at school or in other locations.

- Using profanities, obscenities or offensive language, or using another person's identity by purporting to be that person when, for example, sending emails or interacting on social media

- Attacking people on the grounds of race, religion, race, colour, national origin, disabilities, gender or sexual persuasion or in any other way.

- Harassing other people, for example, by using a network in a way that bothers them and not stopping when asked to do so.

Revised December 2017. No changes made.
Next Revision December 2019