BRACKEN RIDGE STATE HIGH SCHOOL

Policy for Users of Information Technology

INTRODUCTION

Bracken Ridge High School provides Information Technology resources and access to Local Area Networks, Wide Area Networks, the Internet and a school Intranet in an effort to help support its primary objective which is to enhance learning and teaching in a supportive school environment.

As responsible members of the Bracken Ridge community, it is expected that all students and other members of Bracken Ridge High School will follow and adhere to the guidelines established below. These guidelines are based on the common sense, common decency rules established by Bracken Ridge High School, and laws established by the State of Queensland, and the Commonwealth of Australia. Strict adherence to the following guidelines will help ensure a positive, supportive and productive learning environment for all students.

REQUIREMENTS

All students using Information Technology at Bracken Ridge High School are expected to:

- Respect others' right to freedom from harassment and intimidation.
  - Abusive, threatening, or clearly unwarranted behaviour is offensive and will not be tolerated.
  - Reasonably allow others to work uninterrupted.
  - Clearly and correctly identify yourself in all communications using Information Technology.

- Use the network only for **school related tasks**. Students **MUST NOT BE INVOLVED** in any of the following **prohibited activities.**
  - Downloading or copying of any file that is not for a school related task (i.e. research for an assignment or an in-class activity).
  - Downloading, installing or copying of any executable files, games, MP3s, etc. without the express permission of the HOD of Technology.
  - Creating, saving or using files that are not related to school work. N.B. Students are responsible for all files found on their 'H' drive and/or their own personal USB drives. All students must regularly check their drives to ensure that there are no inappropriate files.
  - Saving files to <u>any drive</u> other than your own 'H' drive.
  - Playing of games, music, videos, etc, unless specifically directed to by the teacher.
  - Tampering with computers, screens, keyboards, mouses, printers, furniture, cabling, power cords etc.
  - Bringing CDs or DVDs to school to use with any school computer without the express permission of the HOD of Technology.
  - Taking ownership of files.
  - Accessing instant messaging services (eg MSN messenger)
  - Accessing chat lines.
  - Creating ZIP files.
  - Sending messages across the network.
  - Excess printing.
  - Accessing the dos prompt.
  - Advertising, selling or purchasing any items.
  - Soliciting, responding to or discussing any illegal actions.
  - Attempting to bypass Education Queensland's filter system.
  - Retrieval, viewing or posting of any inappropriate material, on the network, through email, Facebook, etc. This may include material that is offensive or obscene, or sexually or violently explicit.
  - Use of inappropriate Web blogs.
  - Any other inappropriate activities.
  - Sending any form of spam.

- Use the Internet for purposes that are legal and appropriate.

- Respect and adhere to the laws concerning copyright and other intellectual property rights.
  - Copying files belonging to another user without their express permission may constitute plagiarism or theft.
  - When using information from other sources, students must ensure that it is acknowledged in an appropriate manner. (Correct referencing techniques are available from the school Diary and staff.)

CYBER BULLYING

Cyber bullying and other cyber-safety issues may affect the good order and management of the school where it involves:

- Bullying between children who attend the school,
- Images or videos of children on the school premises
- A student at the school possessing or distributing offensive video, images or texts while at school
- School ICT resources being used

If an online incident impacts on the good order and management of the school, the school may:

- Apply disciplinary action, including suspension and/or a proposal to exclude by the Principal
- Report the incident to the police

It is the responsibility of parents to monitor and manage their child's activities on social networking sites.

NETWORK SECURITY

Students must adhere to the following security restrictions for all systems and information:

Passwords must be kept secret. Students must not share passwords or log other students onto the network or Internet as themselves. The expectation is that you do not share your password with others nor do you allow others to use your account.

- Students must not use any 'USERNAME' or 'PASSWORD' other t
- han their own.
- Never try to evade, disable, modify or 'crack' passwords.
- Respect all security provisions on the system. Computer settings such as desktops, printers, page setups, Internet settings etc. must not be changed.
- Reasonably protect computers and software from viruses and file damage of all types.

The contents of students' home directories are not private and may be inspected by any member of staff without warning or notification. Files that are not related to school work and zip files will be deleted without warning or notification. Student emails sent via the Education Departments mailing system are not private. The Administration and staff have the right to view student emails.

Students are to check their computer, keyboard and mouse at the beginning of every lesson. All problems are to be immediately reported to the teacher.

Violations of these requirements may result in immediate suspension of your Information Technology privileges for a period of at least one week. The Technology Committee and Administration will determine any further action. (This may include students moving up a level in the behaviour management process.) Education Queensland, State or Federal authorities may take further disciplinary actions.

Students who violate these requirements may be suspended from the school for three days. Each further infringement may result in a further suspension.

Students who continue to offend may be permanently denied access to the school network.

*N.B.: Students will not be granted access to the network until the Information Technology Agreement has been returned to the school.

PRINTER USAGE

Students will be provided with the following allocation for printing (half will be allocated first semester and the other half second semester):

- Years 7, 8, 9 - $5.00 - 100 black and white printouts,
- Years 10, 11, 12 - $8.00 – 150 black and white printouts.

Once the allocation has been exhausted, students will be denied access until a minimum payment of $2.00 is made to the Accounts Officer. Any unused printing credit is lost at the end of the school year.

INTERNET USAGE

There will be a limit of 750Mb/month for all students. Should a student exceed this limit they may be given a small allocation until the end of the month. This will be at the discretion of the Head of Department (Technology).

Any questions about this Policy should be brought to the attention of the Head of Department (Technology) or the Principal.

Mrs R Garrick
Principal

Mr K McCahon
Head of Department (Technology)

BRACKEN RIDGE STATE HIGH SCHOOL

Information Technology Agreement

I, _____ , of class _____ have read and understand the Policy for Users of Information Technology and agree to adhere to all of the provisions.

I understand that the Internet Service Provider the school subscribes to is a common carrier of public network content and that Bracken Ridge State High School makes NO WARRANTIES whatsoever relating to the suitability or educational appropriateness of that content.

Further, I affirm that I understand that my access to the school Local Area Network and Wide Area Network such as the Internet, is a revocable privilege, not a right.

I PROMISE to observe all rules and guidelines and to refrain from any language or behaviour that is inappropriate to the network community or the school environment.

I understand that any violations of the above mentioned policy may result in immediate suspension of my Information Technology privileges, and that, as a result of such violations, further disciplinary measures may be taken.

I further understand that violations of the Technology Policy may result in my suspension from the school for three days and each further infringement may result in a further suspension.

I am aware that if an online cyberbullying incident impacts on the good order and management of the school, the school may take disciplinary action including suspension and/or proposal to exclude made by the Principal or report the incident to the police.

I also acknowledge that after I have used my allocation of free printing access provided by the school, I will need to prepay for any further access to these facilities.

I am aware that I will not be granted access to the network until this agreement is returned to the school.

Student's Signature:_____ Date:_____

I, _____, am the parent/caregiver of the above named student. I have read and understand the abovementioned guidelines and I hereby give permission for my son/daughter to use the Information Technology services provided by Bracken Ridge State High School and understand that he/she is required to follow the guidelines.

I further understand that there is a potential for my son/daughter to access information on the Internet that is inappropriate for school students and that every reasonable effort will be made on the part of the staff of Bracken Ridge State High School to restrict/monitor access to such information, but that my son/daughter is ultimately responsible for restricting himself/herself from inappropriate information.

Parent's/Caregiver's Signature:_____ Date:_____