ICT & SAFETY ACCEPTABLE USE POLICY

LUCINDALE AREA SCHOOL

Government of South Australia
Department for Education

The comprehensive computer network at Lucindale Area School supports the teaching and learning program and is intended to extend students' learning. As a student of Lucindale Area School, access to the computer network will enable students to complete course work and develop skills using our IT resources.

Responsibilities

Each student has a responsibility to take care of the computing resources and use them in a careful and constructive way.

It is essential that students:

- logon to the network using their own account only
- leave all equipment in place unless they have teacher permission to do otherwise
- report equipment problems - do not tamper with systems settings, switches, buttons or cables

User Name and Password

Each student will be allocated an EdPass account (User Name and password) to access the network resources. This will give the user access to:

- all networked printers
- the internet through a high speed filtered connection
- personal (electronic mail) email account

The password protects storage space and Internet access. Its confidentiality is a students responsibility and it must not be divulged it to anybody. The school maintains comprehensive monitoring and logging procedures. To ensure security, integrity and responsible use of the resources and as part of maintenance, systems management will monitor all student activity, particularly Internet activity.

USB, Flash Drives, External Drives and Viruses

Flash drives are a major source of viruses into the network. You should use a flash drive ONLY if you need to transfer school-related work files to and from home for further development and as a backup. Flash drives can be unreliable. All our files may be checked for virus contamination before they are opened. Management reserves the right to check any flash drives within the school and confiscate those that pose a threat to the performance of our resources.

The school updates its virus software very regularly but gives no guarantee that it is 100% virus free at any point in time. If students use a flash drive on the school network, they may be asked to display the contents to Systems Management.

The Internet

Use of the Internet has become an integral part of our teaching and learning programs. The Internet is available from networked computers in the school through a highspeed content filtered connection. It should only be used during class time for the completion of research and assignments. Students are expected to work within the guidelines set out by the subject teacher.

The school has implemented a comprehensive monitoring and management infrastructure for Internet access. All Internet access, will be logged against a user's ID. This is an important reason students should ensure their password is never divulged to anyone.

- Students are only permitted to use the supplied e-mail client to send and receive e-mail.
- Students will not access sites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or is illegal in any way.
- Download volumes will be monitored so that bandwidth is only used for school related content.

Engaging in chat lines and/or downloading programs is ONLY allowed at direction of class teachers. Inappropriate use of the internet is a serious matter and can have significant consequences, eg sending a message over the Internet using someone else's name may be a criminal offence.

Sanctions

Students who are found to be using the computing facilities in an unacceptable way will be dealt with according to the Behaviour Management Policy.

Students must understand that:

- They must never change or alter in any way, technical, network, IP address information, MAC Address info or the like
- Their passwords MUST remain confidential and NOT be used or acquired by any other student
- They will not use another student's password to access IT resources
- They are responsible for the content of storage space
- All Internet activity will comply with the standards outlined in this policy
- Failure to use the computing resources properly will be dealt with according to the "Behaviour Management Policy" and will at least result in access privileges being withdrawn.
- Computer activity is monitored
- They will not install or store any program files onto school computers
- They are not permitted to download programs, music, video or view inappropriate material
- They are not permitted to play games on school computers unless at the direction of teachers
- Their external storage device may be confiscated if it contains any files that are not appropriate
- They are not permitted to use networking to store and access files in any other way than via their server space using my login and password
- Ultimately, they are responsible for ensuring their files are safe, accessible and available by subject deadlines

Useful sites:

http://www.cybersafetysolutions.com.au
http://www.acma.gov.au
http://www.kidshelp.com.au
http://www.bullyingnoway.gov.au