ICT NETWORK POLICY
(INTERNET, INTRANET AND EXTRANET)

Everton Park State High School offers students access to a computer network for learning and the storage of personal data files. The Network also provides access to electronic mail and the Internet which enables students to explore thousands of libraries, databases, museums, and other repositories of information and to exchange personal communication with other Internet users around the world.

Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or offensive. While the intention of the school is to use Internet resources for constructive educational goals, students may find ways to access other materials despite our blocking procedures. We believe that the benefits to students from access to the internet in the form of information resources and opportunities for collaboration exceed the disadvantages. However, ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To gain the right to use e-mail and the Internet, all students must obtain parental permission and students must agree to abide by the Rules of Appropriate Use as outlined below.

What is expected?

Students are responsible for appropriate behaviour on the school's computer network just as they are in a classroom. Communications on the network are often public in nature. The use of the network is a privilege, not a right, and may be revoked if abused. The student is personally responsible for his/her actions in accessing and utilising the School's computer resources. Students are advised never to access, keep, or send anything that they would not want their parents or teachers to see. Whenever a student does something on a network they leave little "electronic footprints".

Rules of Appropriate Use

To prevent the loss of the network, Internet, and/or e-mail privileges must be followed:

- Respect the opportunity Everton Park State High School provides to use modern and expensive computer networks for your education.
- Use the system only for educational and career development activities and very limited, high-quality, self-discovery activities. There is no limit on use for education and career development activities. The limit on self-discovery activities will be set as necessary by supervising teachers and support staff.
- Ask permission from a teacher BEFORE connecting any external storage or other device to the network (including floppy disks, USB drives, digital devices, etc).
- Report any misuse of the computer network to school staff if they are made aware of it. Failure to do so may be viewed as collaboration. Misuse includes vandalism and theft, possible breaches of security and inappropriate use of the Internet.
- Check e-mails frequently if they have been allocated an e-mail account, and delete unwanted messages promptly, staying within the e-mail quota. Subscribe only to high quality discussion group mailing lists that are relevant to education or career development.
- Be prepared to be held accountable for their actions and for the loss of privileges if these rules are violated.

Students MUST NOT ….

- Enter a computer room or use a School computer without a teacher's permission, knowledge or presence.
- Intentionally explore areas of the network apart from areas accessible in the home folder.
- Copy files to or from any folder on the network, nor to or from any storage device (e.g. Floppy disk, USB drive, CD writer etc) unless directed by your teacher.
- Enter Internet chat rooms, online game sites or online E-mail services (e.g. Hotmail) unless specific permission has been given by a supervising teacher or support staff member.
- Damage computers or the network in any way, nor attempt to gain unauthorised access to any part of the School's computer systems. "Hacking" will not be tolerated.

- Move or remove computers and/or computer parts from a computer room unless specific instructions have been given by a supervising teacher.
- Interfere with the operation of the network by installing illegal software, shareware, or freeware. Anyone found with "hacking" software in their possession or in their personal folders will be considered as having breached network security and will be dealt with severely.
- Violate copyright laws by using material from Internet sites without permission of the copyright owner.
- Plagiarise works that is located on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
- View, send, store or display indecent and/or offensive messages or pictures.
- Use profane, abusive, impolite or sexually explicit language to communicate. Do not knowingly access materials which are not in line with the rules of School behaviour. A good rule to follow is to never view, send, or access materials which they would not want their teachers and parents or colleagues to see. Should a student encounter such material by accident, they should report it to your teacher immediately.
- Share their password with another person or logon for another person whose privileges have been withdrawn.
- Waste limited resources such s disk space or printing capacity. Large files are not to be downloaded unless permission has been obtained from a supervising teacher. Users are expected to remain within allocated disk space and delete material which takes up excessive storage space.
- Trespass in another's folders, work, or files. Respect their privacy. Network storage areas may be treated like school lockers. The Information Technology Coordinator may review communications to maintain system integrity and will ensure that students are using the system responsibly.
- E-mail, or place on the Web, personal contact information about themselves or other people. Personal contact information includes their home address, telephone number, the school address, your work address etc.
- NEVER agree to meet with someone they have not met online unless they have their parent's approval.

Possible Network misuse will be detected in a number of ways:

- As reported by staff or students
- As notified by Education Queensland Officers (Note: Education Queensland reserves the right to monitor and audit any or all intranet, Internet or e-mail activity undertaken by EQ officers using departmental resources.
- As discovered by the Information Technology Coordinator through for example, inspection of Network security logs and Internet proxy logs, scans of student file storage areas, and automatic notifications of inappropriate e-mail use.

Student Web Pages

Students may be asked to establish personal Web pages for sound educational reasons for a unit of work in certain subjects. A process and criteria for the establishment and posting of material, including pointers to other sites, on these pages will be available before publishing. Material presented in the student's Web site must be related to the student's educational and career preparation activities.

Student Web pages must include the following notice:

"This is a student Web page. Opinions expressed on this page shall not be attributed to Everton Park State High School or to Education Queensland."

All students and a parent/guardian must sign the User Agreement Form to be granted access to the Internet and/or an individual e-mail account on the School network. This Agreement must be renewed on an annual basis.

Clearing of School Computer Accounts

The H Drive of the student's computer at school will be cleared out at the end of each term. It is the student's responsibility to transfer any information that they want to keep prior to the end of term.

CONSEQUENCES OF RULE VIOLATION

Consequences of a rule violation for the student concerned may include immediate suspension from the School, suspension from Network access, and/or removal from computer-related subjects. Any action will be determined by the Information Technology Coordinator in consultation with the Principal, Deputy Principal and/or Heads of Department.

Disciplinary consequences for various rule infringements are as follows:

Rule Violation	Consequences	
	1st Offence	2nd Offence
Inappropriate visits to Internet sites deemed outside the scope of "educational and career development activities and very limited, high-quality, self-discovery activities".	Internet access withdrawn for four weeks without warning. Students will still have access to all school-based computer resources, but they will not be able to use the Internet.	Internet access withdrawn for four weeks. One afternoon detention Warning letter that next offence will warrant permanent withdrawal of internet access
Visits to pornographic sites and/or download of pornographic pictures.	Internet access withdrawn for four weeks One afternoon detention Parent interview Warning letter	Permanent withdrawal of Internet access Recommendation for exclusion from the School
Download of files in breach of the Rules of Appropriate Use OR installation of games on network or local computer hard drive via Internet.	Internet access withdrawn for two weeks without warning Offending files deleted without warning	Internet access withdrawn for four weeks without warning Offending files deleted without warning Warning letter to parents[1]
Upload of inappropriate files to network OR installation of games on network or local computer hard drive via floppy or CD.	Internet access withdrawn for two weeks without warning Offending files deleted without warning	Internet access withdrawn for four weeks without warning Offending files deleted without warning Warning letter to parents[1]
Minor attempts to gain unauthorised access to any part of the Network systems (e.g. Use of another's login)	Network access withdrawn for two weeks Warning letter	Network access withdrawn for four weeks One afternoon detention Parent Interview Removal from subjects
Major attempts to gain unauthorised access to any part of the Network systems e.g. Via hacking, 'spyware' or other "backdoor" methods **OR** the use of the teacher or network manager logins **OR** copying and/or misuse of school data.	Twenty-day suspension from school or exclusion Removal from subject Network access withdrawn for rest of year Notification of School-Based Police Officer	Recommendation for exclusion from the School
Wilful damage to computers or attempts to cause harm to the Network	As per School policy for wilful damage	
Entry into computer labs or pods without teacher permission /supervision	One afternoon detention	
Theft of computer equipment	As per School policy for theft	

[1] PLEASE NOTE: warning that next offence may result in change of subject and/or withdrawal from subject and permanent withdrawal of network and/or Internet access.