

RONDEBOSCH BOYS' HIGH SCHOOL

USE OF INTERNET AND ELECTRONIC MAIL – PERMISSION FORM

Rondebosch Boys' High School is proud to offer learners access to a computer network for Electronic mail and the Internet. To gain access to e-mail and the Internet, all learners must obtain parental permission as verified by the signature on the form below.

Should a parent prefer that a learner not have e-mail and Internet access, use of the computers is still possible for more traditional purposes such as word processing.

What is possible?

Access to e-mail and the Internet will enable learners to explore thousands of libraries, databases, museums and other repositories of information and to exchange personal communication with other Internet users globally. Families should be aware that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive.

We have installed software to restrict access to unsavory sites, but as the Internet changes by the minute, it is not always possible to know every web site that could be problematic.

While the purposes of the school are to use the Internet resources for constructive educational objectives, Learners may find ways to access other materials. We believe that the benefits to learners from access to the Internet in the form of information resources and opportunities for collaboration exceed the disadvantages, but 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.

Therefore, we support and respect each family's right to decide whether or not to apply for access.

What is expected?

Learners are responsible for appropriate behavior on the school's computer network just as they are in a classroom or on the school playing fields. Communications on the network are often public in nature. General school rules for behavior and communications apply. It is expected that users will comply with standards and specific rules set forth below. The use of the network is a privilege, not a right, and may be revoked if abused. The school's computer resources are to be utilized for educational purposes only. The user is personally responsible for his actions in accessing and utilizing the school's computer resources. Learners are advised never to access, keep and or send anything that they would not want their parents or educators to see.

What are the rules?

Privacy – Network storage areas must be treated like school lockers. Network administrators have the right to monitor, record, take control and review communications of any student(s) computer on the school network to maintain system integrity while ensuring that learners are using the system responsibly. Students will be informed and updated on a regular basis which site(s) they may not view. The network administrator(s) have the right to scan and check any media storage device that is use on the school network to maintain system security and integrity.

Storage capacity – Users are expected to remain within allocated disk space and delete excessive or obsolete files and material from their folders.

Illegal copying – Learners should never download or install commercial software, freeware or shareware onto network drives or disks, unless they have written permission from the Network Administrator. Nor should learners copy other people's work or intrude into other people's files.

Completed Form to be returned via class teachers to the IT Manager - 2008

Learners Agreement to Comply with Acceptable Policy

As a user of the School computer network, I agree to comply with the above stated rules and to use the network in a constructive manner.

Learner's Full Name (print) _____ Grade _____

Learner's Signature _____

Date: _____

Parents Permission Form and User Agreement

As a parent or guardian of a learner at RBHS, I have read the above information about the appropriate use of computers at the school and I understand this agreement will be kept on file at the school.

My son may use e-mail and the Internet while at school according to the rules outlined.

Or

I would prefer that my son not use e-mail and the Internet while at school.

(Delete whichever is not applicable)

Parent/Guardian Name (print) _____

Parent/Guardian Signature _____

Date: _____

Parents Permission for the Publication of Learners Pictures and or Work

I understand that from time to time RBHS may wish to publish examples of learner's projects, other work and or pictures of school activities in which my son might appear on the school Web site (www.rbhs.co.za) This Web site is accessible on the World Wide Web to all Internet users.

My son's work can be published on the Internet.

Or

I would prefer that my son's work not be published on the Internet.

(Delete whichever is applicable)

Picture of school activities in which my son might appear may be published on the Internet.

Or

I would prefer that pictures that my son appears in not be published on the Internet.

(Delete whichever is applicable)

Parent/Guardian Name (print) _____

Parent/Guardian Signature _____

Date: _____

MISUSE AND INAPPROPRIATE BEHAVIOUR

The following activities are expressly prohibited:

1. Using a computer system without proper authorisation granted through the school. Activities include “port scanning”, which is expressly prohibited unless undertaken by IT administration as part of security measures to enforce network integrity.
2. Concealing one’s identity or assuming the identity of another, e.g. sending forged electronic messages. Note that some forms of electronic communication, such as browsing web pages, passively “identify” users. Keeping one’s identity private, either by not setting an identity in one’s browser or by using a web-anonymiser in order to protect one from being put onto mailing lists, is not a violation of this policy.
3. Sharing passwords or account data.
4. Using another person’s computer account, logon ID, files or data without appropriate permission, as described in the previous bullet.
5. Deleting or tampering with another user’s files or with information stored by another user on any information-bearing medium (disk, tape, memory, etc.). Even if the user’s files are unprotected, with the exception of files obviously intended for public reading, such as web pages, it is improper for another user to read them unless the owner has given permission, e.g. as an announcement to a class.
6. Attempting to “crack” or guess other users’ passwords. System administrators or those specifically designated by the administrator or owner of a system may attempt to crack passwords in order to test and enhance the security of the system. In cases where an individual or department “owns” machines, which use password files controlled by another, the owner may not attempt to crack passwords without explicit permission by the owners of the password database.
7. Obtaining passwords by other means, such as password capturing programs.
8. Attempting to circumvent system security (e.g. breaking into a system or using programs to obtain “root” access) without the explicit permission of the owner of that system.
9. Denying appropriate access to resources to other users, e.g. “ping flooding” another system, sending “mail bombs” or modifying a login file in order to disable a user to log in.
10. Releasing programs such as viruses, Trojan horses, worms, etc., that disrupt other users, damage software or hardware, disrupt network performance, or replicate themselves for malicious purposes.
11. Sending commercial solicitations via electronic mail (i.e. spamming) to individuals or distribution lists in the school.
12. Any “mass mailing”, which is solicitous in nature, unless the mailing is in the conduct of school business.
13. Running a proxy server which results in inappropriate or unauthorized access to school materials.
14. Using mail messages to harass or intimidate another person, such as repeatedly sending unwanted mail or broadcasting unsolicited mail.
15. Violations of any laws, such as the distribution of copyright-protected materials, e.g. the distribution of commercial software, music or films in electronic format without appropriate permission by the owner, even if the user distributing the materials notifies others of their copyright status.
16. Tampering with, willful destruction of or theft of any computer equipment, whether it belongs to the school or to an individual. Tampering includes any deliberate effort to degrade or halt a system, to tie up a system or to compromise the system/network performance. Willful destruction includes any deliberate disabling or damaging of computer systems, peripheral equipment such as scanners or printers, or other facilities or equipment including the network, and any deliberate destruction or impairment of software or other users’ files or data.
17. The unauthorized removal of school, staff or student computing equipment, which constitutes theft.
18. Do not change or modify any aspects of the computer hardware or software that will alter how the system appears or operates, including accessing control panels or other computer settings and changing anything on the desktop, hard drive or network.

Inappropriate or language – Profane, abusive or impolite language should not be used to communicate nor should materials be accessed which are not in line with the rules of school behaviour. A good rule to follow is never view, send or access materials, which you would not want your parents or educators to see. Should learners encounter such material by accident, they should report it to their educator immediately.

Succinct Advice

1. Do not use a computer to harm other people or their work.
2. Do not store or use any harmful material or software on the server or on any means of storage device e.g. viruses
3. Do not damage the computer or network in any way.
4. Do not interfere with the operation of the network by installing illegal software, shareware or freeware.
5. Do not violate copying laws.
6. Do not download or play games, videos and music.
7. Do not send, view or display offensive messages or pictures.
8. Do not share your password with other people.
9. Do not waste limited resources such as disk space or printing capacity.
10. Do notify an adult immediately, if by accident, you encounter materials, which violate the rules of appropriate use.
11. Do not trespass in one another’s folders or work.
12. BE PREPARED to be held accountable for your actions and for loss of privileges if the “Rules of Appropriate Use” are violated.

Some Useful Links that you might want to visit:

www.safekids.com
www.weblinksresearch.co.za

Search engines for children:

www.wikipedia.org/
www.ivyjoy.com/rayne/kidssearch.html
www.askjeeves.com
www.google.co.za
www.ananzi.co.za

Other interesting sites

www.rondebosch.com
www.rbhs.co.za