

COMPUTER AND INTERNET POLICY



General Guidance

You are responsible for all accounts under your name. You must not disclose your password(s) to anyone, if you suspect a password has been discovered by another person you must change it immediately. Your printing credits are protected by the security of your account, refunds will not be given for lost credits caused by others gaining access to your account. When you leave your machine you are responsible for ensuring that you are logged out effectively.

All computers within the School have a virus protection system installed. You must not interfere with the operation of this system.

The holding or distribution of computer files containing obscene or offensive material will be treated as a serious breach of these conditions unless explicitly authorised as part of an academic study.

You are not allowed to take into any area of IT equipment any forms of entertainment, which may interfere with other users. The taking of food and drink into these areas is not permitted.

All mobile phones should be switched off before entering an IT area.

Unreasonable behaviour (for example using facilities for games, chats etc. when others cannot access a system to carry out study related work) will not be tolerated.

Unruly behaviour between students or towards ArtsEd staff is considered a serious offence.

Before connecting any device (e.g. a laptop) to the School network you must obtain authorisation, this procedure will normally require details such as the network address of the unit being recorded and for you to agree to be responsible for activity initiated from the unit. If the unit does not belong to the School you are responsible for protecting the unit against computer viruses and similar threats.

You are expected to use the School IT facilities for School related activities, limited personal use is allowed provided that it does not prevent others from pursuing their legitimate work.

The use of IT facilities for significant personal financial gain or any unlawful activity (such as storing obscene material) will be considered a serious offence.

Electronic Mail

1. No e-mail may be sent or forwarded through the School system for purposes that violate School regulations or for an illegal or criminal purpose.
2. Electronic mail, like user files, is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness. The School and its Administrator of central e-mail systems will not read mail unless necessary in the course of their duties. Also, there may be inadvertent inspection in the ordinary course of managing and maintaining the computer network and in carrying out other day-to-day activities.
3. Nuisance e-mail or other online messages such as chain letters, obscene, harassing, or other unwelcome messages are prohibited.
4. Unsolicited e-mail messages to multiple users are prohibited unless explicitly approved by the appropriate School authority. All messages must show accurately from where and from whom the message originated, except in the rare, specific cases where anonymous messages are invited.

The School reserves the right to refuse mail and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses to School or other users, and to filter, refuse or discard such messages.

Network Security and Privacy Policies

1. Unauthorized attempts to gain privileged access or access to any account or system not belonging to you on any School system are not permitted.
1. Computer and network accounts provide access to personal, confidential data. Therefore, individual accounts cannot be transferred to or used by another individual. Sharing accounts or passwords is not permitted.
2. Each user is responsible for the proper use of his or her account and any activity conducted with it. This includes choosing safe passwords, protecting them, and ensuring that file protections are set correctly.
3. Each system owner is responsible for the security of any system he/she connects to the network. A system seen to be attacking other systems, e.g. having fallen victim to viruses/worms, will be taken off the network, generally without notice, until it has been made secure.
4. No School system or network may be used as a vehicle to gain unauthorized access to other systems.
5. Any user who finds a possible security lapse on any School system must report it to the system Administrator. To protect your files and the system, don't attempt to use a system under these conditions until the system administrator has investigated the problem.
6. All users should be aware that the system administrator conducts periodic security checks of School systems, including password checks. Any user found to have an easily

guessed password will be required to choose a secure password during his or her next login process.

7. User files on central School systems are kept as private as possible. Attempts to read another person's protected files will be treated with the utmost seriousness. The system Administrator will not override file protections unless necessary in the course of his duties, and will treat the contents of those files as private information at all times.

Network and Computing Usage Policies

1. No School system may be used for purposes that violate School regulations, or for illegal or criminal purposes.
2. Please keep in mind that many people use School systems for daily work. Obstructing this work by consuming gratuitously large amounts of system resources (disk space, CPU time, print quotas, and Network bandwidth) or by deliberately crashing the machine(s) will not be tolerated.
3. Use of any School system by outside individuals or organizations requires special permission from the system's administrator.
4. Use of School systems for commercial purposes, except where explicitly approved, is strictly prohibited. Such prohibited uses include, but are not limited to, development of programs, data processing or computations for commercial use and preparation and presentation of advertising material.
5. No School computing facility may be used for playing computer games.
6. Copying, storing, displaying, or distributing copyrighted material using School systems or networks without the express permission of the copyright owner, except as otherwise allowed under the copyright law, is prohibited.

Violations of these policies may result in the immediate suspension of computer account and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations of the policy will be referred directly to the appropriate School or outside authorities; unauthorized use of School computing facilities can be a criminal offence. The penalties may be as severe as suspension or dismissal from the School and/or criminal prosecution.

Password Policy

The combination of username and password define the identity of users on a system.

Content

* Mixture of numbers, capital letters, small letters, punctuation.

- * Easy to remember (don't need to write it down).
- * Easy to type quickly (difficult for an observer).

Examples

- * Choose a line or two of a poem, song etc. and use just the first letters.
- * Join two small words with a strange character.
- * Invent an acronym.

Bad examples

- * Name of your spouse, parent, colleague, friend, pet, towns, months, days.
- * Number of car/motorbike registration, telephone.
- * Common dictionary words (French, German, English, Italian..).
- * A series of identical numbers/letters.
- * Obvious keyboard sequences.
- * Any of the above in inverse or with a number before or after.

Guidelines

- * Don't write it down, or disclose via email.
- * Default passwords should not be used.
- * Don't give your password to others.
- * If passwords are disclosed on a system, change them immediately.