



INFORMATION TECHNOLOGY DEPARTMENT

Rules Governing the Use of IT Facilities

The Cagayan De Oro College is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative and service functions. The College has adopted IT policies, which define the acceptable behavior expected of users and intending users of the facilities.

The following rules are an extraction from the IT policies. The College requires users to accept the IT policies and associated rules governing the use of the IT facilities as a condition of their use. The Cagayan De Oro College IT facilities are provided to assist staff, students and other authorized users to conduct bonafide academic and administrative pursuits.

1. Only authorized users may use the facilities and a user may only use those facilities to which they are authorized.
2. All users must accept full responsibility for using the School's IT facilities in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people. Use must be in accordance with School policies and all relevant republic legislation.
3. Where access to a facility is protected by an authentication method, e.g. a password, a user must not make this available to any other person. Users who do so will be held responsible for all activities originating from that account. A user must not use an account set up for another user nor make any attempts to find out the password of a facility they are not entitled to use. A user can expect that access to their account shall not be available to another user. A user must not attempt to find out the authentication secret of any other user. The above does not apply where a user provides access to their account to an authorized support person. The School discourages the storing of passwords due to the security risks this poses.
4. Each user, while using their account, is responsible for:
 - a) All activities that originate from their account;
 - b) All information sent from, intentionally requested, solicited or viewed from their account;
 - c) Publicly accessible information placed on a computer using their account.
5. School IT policy requires that users:
 - a) Show restraint in the consumption of resources;
 - b) Apply academic and professional integrity;
 - c) Respect intellectual property and the ownership of data and software;
 - d) Respect other's rights to privacy and freedom from intimidation, harassment and annoyance;
 - e) Shall not attempt to subvert the security of any of the School's IT facilities;
 - f) Shall not attempt to create or install any form of malicious software (for example worms, viruses, sniffers) which may affect computing or network equipment, software or data;
 - g) Shall not attempt to interfere with the operation of any of the School's IT facilities;
 - h) Shall not attempt to subvert any restriction or accounting control of any of the School's IT facilities;
 - i) Shall not attempt unauthorized access to any School IT facilities;
 - j) Shall not use the School IT facilities for private gain or for financial gain to a third party;



INFORMATION TECHNOLOGY DEPARTMENT

Rules Governing the Use of IT Facilities

6. The School Network and IT facilities, including email and web servers and other similar resources, may not be used for:
 - a) The creation or transmission (other than for properly supervised and lawful teaching or research purposes) of any material or data that could reasonably be deemed offensive, obscene or indecent;
 - b) The creation or transmission of material which the average person deems likely to harass, intimidate, harm or distress;
 - c) The creation or transmission of defamatory material;
 - d) The transmission of material that infringes the copyright of another person;
 - e) The unauthorized transmission of material that is labeled confidential or commercial in confidence;
 - f) The transmission of any material that contravenes any relevant federal or state legislation;
 - g) The deliberate unauthorized access to facilities or services.
7. Users are responsible for making use of software and electronic materials in accordance with the Copyright Act 1968, software licensing agreements, and any applicable School policies.
8. A user must not examine, disclose, copy, rename, delete or modify data without the express or implied permission of its owner. This includes data stored on storage devices and data in transit through a network. A user must respect the privacy and confidentiality of data stored or transmitted on the School's IT facilities. Any release of data to those not authorized to receive it is expressly forbidden.
9. Users must take due care when using IT equipment and take reasonable steps to ensure that no damage is caused to IT equipment. Users must not use equipment if they have reason to believe it is dangerous to themselves or others to do so and must report any damage to IT equipment to appropriate personnel. No user shall without proper authorization:
 - a) Attach any device to School IT facilities;
 - b) Connect any equipment to the School network (for example a modem) that will extend access or provide off-campus access to School IT resources without the prior written approval of the Director (ITS) or delegated persons, that such connection meets School security standards;
 - c) Tamper with or move installed IT facilities without authorization.
10. A user of a computer laboratory shall abide by any instruction or signage as provided by authorized personnel and shall provide relevant identification on request. The School reserves the right to apply additional policy and rules specific to individual laboratories.

The School treats misuse of its IT facilities seriously. Violations of the conditions of use of IT facilities will be dealt with as specified under IT policy compliance.