NCAD DUBLIN
National College of Art and Design
A Recognised College of University College Dublin

Computer & Network Systems
Acceptable Use Policy & Code of Conduct

		This policy is effective from	July 2012
Approval body	College Management Team	**Approval date**	Prior to July 2012
Owner	Registrar	**Next review date**	June 2018

1. Introduction

1.1. The National College of Art & Design is anxious to achieve a balance between proper and legitimate academic and personal usage of computers and the College's responsibility to monitor and regulate any misuse whilst still maintaining the individual's legitimate privacy.

1.2. The College is committed to providing computer resources including email and internet access for staff and student use to promote the aims of the College's programmes and to facilitate education, research and administration.

1.3. Through the College's IT Committee the following usage policies have been established to ensure that the College can offer the widest possible range of services to the College community without limiting academic freedom.

1.4. The College is committed to maintaining the privacy of its users and will not actively monitor computer usage, but users should be aware that the College will be retaining records of all usage and these records could be made available in specific circumstances.

1.5. The College's computer resources may not be used:

1.5.1. For illegal acts

1.5.2. For activities in breach of College policies

1.5.3. For personal commercial activity (unless specifically authorised by the IT Committee)

1.6. The College computer facilities are only available for the College community.

1.7. All users carry duties and responsibilities in relation to computer and network systems and must adhere to the following broad policies:

1.7.1. All users must respect the laws of Ireland and specifically but not exclusively be aware of their individual responsibilities under:

1.7.1.1. Copyright Act (1963) and Amendments

1.7.1.2. Data Protection Act (1988)

1.7.1.3. Prohibition of Incitement to Hatred Act (1989)

1.7.1.4. Criminal Damage Act (1991)

1.7.1.5. Freedom of Information Act (1997)

1.7.1.6. Child Trafficking and Pornography Act (1998)

1.7.2. The College will provide all users with an account number and a password to permit access to the College's network and other computer resources. It is the responsibility of the individual member of the College community to prevent unauthorised use of their account. Staff members must ensure as far as practical that the computers, either in their office or under their direct care are not used for unauthorised purposes. The IT Manager will be in a position to give advice and assistance in safeguarding software and equipment.

1.7.3. Users must behave reasonably in their use of the College computer facilities and must not undertake or facilitate any activity that could jeopardise in any way the integrity, reliability and performance of these resources. Users must check with the IT Manager before doing anything that might affect the network. Wilful damage to computer resources will result in disciplinary action which may include prosecution under appropriate legislation. Deliberately wasteful use of resources and time could lead to withdrawal of services or disciplinary action.

1.7.4. Users must take reasonable care to ensure that they do not transmit viruses or other malicious computer codes to other users. The College will provide guidelines and practical help to all users to protect their computers.

1.7.5. It is not acceptable to view, download, transmit or store any offensive indecent images or material unless this is an integral part of the research being pursued by the user and has been agreed in writing with the relevant Head of School and the Director.

1.7.6. It is not acceptable to attempt to access any files, data or records for which the user is not authorised.

1.7.7. The College's computer system is not to be used to publish or transmit anything that is libellous or defamatory or is damaging to another computer system.

1.7.8. Users must clearly indicate that any views that they express whilst using the computer facilities are their own views and not those of the College.

1.7.9. All software installed and used on the College computer systems, including stand-alone computers, must be appropriately licensed. Users must adhere at all times to the terms and conditions of such licenses.

1.7.10. Increasing amounts of data and information are stored on electronic media and the College computer system. Users who have access are responsible for such data and must make themselves aware of the College Computer & Network Systems Code of Conduct and ensure that the integrity, accessibility, accuracy and confidentiality of such data is maintained.

1.7.11. Failure to abide by these policies may result in being denied access to the computer resources as well as other proceedings.

1.7.12. All work for the College website must be approved through the College webmaster and must be approved by the Head of the appropriate area.

1.7.13. This policy on acceptable computer use will be amended from time to time as required. All users of College computer resources are deemed to have made themselves aware of these policies.

2. Code of Conduct

The College has issued a Computer and Network Systems Acceptance Use Policy and this Code of Conduct arises from that policy. The Code of Conduct applies to all users of the computer and network systems in the National College of Art & Design.

2.1. Access to server rooms is strictly forbidden unless authorised by the IT Manager or the Buildings Officer (Facilities Manager).

2.2. Web shots and outside media will be blocked. Requests can be made to the IT Manager through the Head of School/Head of Department to connect to outside media.

2.3. IT equipment should not be taken off site without the authorisation of the Head of School or Head of Department and the IT Manager.

2.4. All equipment which is taken off site must be separately insured through the Accounts office.

2.5. Schools and Departments are required to maintain written records of all software installed in each machine.

2.6. Software:

2.6.1. All software installed on a machine must have a valid license and proof of ownership.

2.6.2. Personally owned software should not be installed on a machine.

2.6.3. When installing software or purchasing new software for a machine the IT Manager must be advised so that School and Department records for each machine are updated.

2.6.4. Users must not copy software or data without the permission of the copyright owner.

2.7. Computer and network resources are not to be used for individual commercial use unless authorised by the College management.

2.8. Connection of devices to the College network is strictly forbidden.

2.9. Use of malicious code programmes is not permitted nor is the intentional destruction or unauthorised monitoring of electrical communication.

2.10. Encryption technology cannot be used on electronic data without notifying the IT Manager in advance.

2.11. Use of a modem on a computer is prohibited without notifying the IT Manager in advance.

2.12. Users must be aware that websites visited and incoming/outgoing emails will be logged by the server. These logs are backed up daily and will be held for a month before being overwritten.

2.13. Disc space may be requested from the IT Manager for staff members to store files.

2.14. Disc space and email accounts will be deleted when a user finishes their connection on a day-to-day basis by the College. This deletion will take place one month after the user leaves the College.

2.15. Authorisation must be sought from the IT Manager for additional network points.

2.16. Users must respect the laws of Ireland and be aware of their responsibilities under Copyright Act (1963) and the following laws as amended.

2.16.1. Data Protection Act (1988)

2.16.2. Prohibition of Incitement to Hatred Act (1989)

2.16.3. Criminal Damage Act (1991)

2.16.4. Freedom of Information Act (1997)

2.16.5. Child Trafficking and Pornography Act (1998)

2.17. In the interests of health and safety the removal of covers from machines is strictly forbidden.

2.18. In the summer period staff can request their account at *ncad.ie* emails to be sent to an outside email address; however it is essential that the address is one where anti-virus software has been installed.

2.19. Schools and Departments that are upgrading their machines and disposing of the old ones must give a list of computers for resale to the IT Manager.

2.20. Users should be aware of the computer users' Health, Safety & Welfare Document recommending suitable positions for computer equipment and furniture.

2.21. All computer equipment that is not working and cannot be fixed will be sent to a designated recycling company for disposal. This must be arranged through the IT Manager.

2.22. Network settings on computers are not to be changed.

2.23. Email: All staff emails will be in the format lastnameinitialoffirstname@ncad.ie.

3. Version history

3.1. Previous document uploaded to website on 31 July 2012.

3.2. This document is the same content in a new template.