Nescot

Student IT Usage Agreement

NESCOT Student IT Usage Agreement

As a Nescot student, you are entitled to use the College's IT facilities. This includes computers, software, multi-media and the College Virtual Learning Environment (Weblearn). It also includes the use of the Internet, including access to online databases, electronic journals, learning materials and private email. All users both staff and students must adhere to the policy below which ensures we have clear rules to make sure that everyone's privacy and rights are respected and that the system continues to work efficiently and it also ensures the College systems are not abused. This policy covers all computers, laptops and electronic devices in the College irrespective of who owns the device.

Please read this document and sign it to say that you agree to the rules. In return, we agree to maintain the system to the best of our ability so that you can use it as you need to.

---

1. You can use the IT network for...

- Work connected with your college course
- Any educational activity
- Communicating responsibly with other students and staff
- Communicating responsibly with outside organisations related to your college course

You cannot use the college network for...

- Spoiling, disrupting or destroying other people's work or their use of the system – e.g. by deliberately introducing viruses, overloading the system.
- Invading anyone else's privacy.
- Hacking or trying to circumvent any security protocols.
- Making or sending anything, which may annoy, inconvenience or upset anyone.
- Making, downloading, sending or receiving anything that is offensive or obscene.
- Sending anything that is covered by copyright policy
- Loading your own software.
- Selling anything to anyone.
- Use abusive, aggressive or defamatory language in all forms of social media or Weblearn
- You should never deliberately install and use software illegally or install any malicious code on the Colleges system.
- You should not eat or drink anywhere there is ICT equipment.
- You may not physically damage, disable or harm ICT equipment.
- You may not use the IT facilities for playing games, or any non-college activity that may cause strain on the device or network, for example, bitcoin mining.
- Connecting personal devices to any network other than Eduroam.

Please tick the box opposite to confirm you have read and understood Section 1	

2. Use of College and External Social Media Applications

We all use social media. Applications like Facebook, Twitter and Instagram help us keep in contact with friends and family. At college, you use Weblearn to communicate with fellow students and teachers. There are some golden rules that you need to consider when using social media applications:

Do not...

- Give out personal information like your address or telephone number.
- Open emails or attachments from people you do not know.
- Become online 'friends' with people you don't know in real life.
- Arrange to meet somebody you have met on-line.
- Send, display, print or download text, images, video or sound, which is offensive or degrading to others based on race, origin, sex, sexual orientation, age, disability, religious or political beliefs.
- Use obscene, racist or degrading language.
- Post confidential information.
- Allow other people to use your college account.
- Produce propaganda for religious or political extremism causes.

Please tick the box opposite to confirm you have read and understood Section 2	

3. Cyberbullying

Most social media users are genuine, but because it is so easy to hide your real identity, it is possible to come into contact, with people you would normally avoid. Cyber bullying can work in the same way as bullying: the victim feels frightened and alone, while the bully tries to hide from being caught. Comments, images and videos about a person can be posted online causing the victim to feel frightened and upset.

Often cyber bullies feel braver because they cannot be seen, but it can be the most traceable form of bullying because there's evidence that it's happened. Because bullies think they can cover up their identity online, sometimes people who would not normally bully might do so online.

Any student who is guilty of bullying either a fellow student or member of staff via college or external applications will be dealt with under the Student Disciplinary process.

Please tick the box opposite to confirm you have read and understood Section 3	

4. E-Safety

I will ...

- Ensure that I am aware of e-safety and how it applies to me and everyone else.
- Report any accidental access to inappropriate material to the ESafety Officer or a member of staff
- Ensure that I do not research any material that references terrorist and extremist material on the internet.
- In compliance with Counter-Terrorism and Security Act 2015 and the Prevent regulations, users must not create, transmit, receive view or store material with the intent to radicalise themselves or others.
- I will not attempt to bypass the Colleges proxy server.
- I will not use the internet to obtain, download, send, print, transmit or access material that is deemed to be unlawful, obscene or abusive.
- I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

Please tick the box opposite to confirm you have read and understood Section 4	

5. Use of Software

Nescot has signed copyright agreements which mean that the software must not be used for commercial or personal use. Software must not be downloaded from the Internet unless you have been given written permission or it is a supervised part of your course.

Please tick the box opposite to confirm you have read and understood Section 5	

6. Use of Copyright Software: Copyright Acknowledgement

I agree that my usage of any Software, Computer Readable Dataset or Courseware or other similar material, hereafter referred to as "the Product", issued or otherwise made available to me by the Institution to which I am a student or member of staff is subject to the following conditions:

- I will ensure that all the requirements of the agreements, contracts and licences under which the Product is held by the Institution will be maintained. (Copies of the relevant agreements, contracts and licences may be seen by application to the School or Department which made Product available.)
- I will adhere to the regulations governing the use of any service involved in the provision of access to the product whether these services are controlled by my own institution or by some other organisation.
- I will not remove or alter the Copyright Statement on any copies of the Product used by me.
- I will ensure the Security and Confidentiality of any copy released to me, and will not make any further copies from it or knowingly permit others to do so, unless permitted to do so under the

relevant licence.
- I will use the Product only for purposes defined, and only on computer systems covered, by the

agreement, contract or licence.

- I will only incorporate the Product, or part thereof, in any work, program or article produced by me, where this is permitted by the licence or by "Fair Dealing".
- I will only incorporate some part or version of the Product in any work produced by me with the express permission of the Licensor or unless this is permitted under the Agreement.
- I will not reverse engineer or decompile the software products or attempt to do so unless this is explicitly permitted within the terms of the Agreement for the use of the Product.

I will return or destroy all copies of the Product at the end of the course/year/period of employment or when requested to do so.

In signing this Copyright Acknowledgement Form I understand that the Institution reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of violation of its licensing agreements.   If you have any questions about the Copyright Acknowledgement please ask at the LRC Help Desk (020 8394 3055)

You should also know that...

- You must comply with Data Protection Act 1998, Computer Misuse Act 1990, Copyright Protection Act 1956, Copyright (Computer Software) Amendment Act 1985, Copyright, Designs & Patents Act 1998 & the Privacy and Electronic Communications Regulations 2011. (Copies are available in the LRC).

- You must comply with the JANET Acceptable Use Policy which can be found on the Jisc website.

In order to protect your work and the work of all other users, we will take very seriously any breach of these rules.

Please tick the box opposite to confirm you have read and understood Section 6	

7. Monitoring

- I understand that all Internet and email usage will be logged and this information could be made available to a member of the Senior Management Team, Safeguarding team or E-Safety officer on request.
- I understand that all files and emails on the system are the property of the College. As such, system administrators have the right to access them if required.
- I understand that all network access, web browsing and emails on the College systems and laptops are logged and may be routinely monitored on any computer screen without a person's knowledge.

Please tick the box opposite to confirm you have read and understood Section 7	

8. User Identification

- All users will be given a unique user account for individual use. This account will be used at the college for use of identification and access to different areas of the IT network.
- Users are responsible for their own network account and any activity associated on that account. You must not use anyone else's account, nor must you allow anyone else to use your account.
- You must not share your account details with anyone else. Anyone asking for your account details are to be considered fraudulent. IT Services will never ask for your password.
- If you believe your account to be compromised, you must change your password straight away. It is recommended that you change your password annually.
- Password security requirements define that you must have a strong password (recommended 11 or more characters long; must contain three of the following character definitions: uppercase, lowercase, number and symbol; must not contain a significant portion of your username and may not be one of the last 4 passwords you have used).
- You must not use the password you have for you NESCOT account for any other purpose be it personal or business use.
- All common or easily guessed passwords are not to be used. Common passwords are passwords that have any relation to the user e.g., pets name etc or easily guessed passwords such as 'Collegename1'.
- It is recommended that you use a passphrase which could be three random words mixed with symbols and numbers to makes it easier to remember. As an example, taking the words Football, School and Sandwich to create FooTball$chool!SandWich%
- You must not write down or store your password in plain text (unencrypted). If you are struggling to remember passwords, then you should look at using a password manager.

9. Remote working/Access

- The college uses some third party hosted applications as well as allows some on site services that can all be accessed outside of the college campus. These services include but are not limited to Office365, Weblearn and GSuite. Users are permitted to uses their own devices to access these applications, but security protocols must be adhered to.
- All remote workers must ensure that the device they are using is up to date with all security packages within 14 days of release and is running a full and up to date malware protection program.
- All devices being used for remote access must be vendor supported. E.g., the support for Windows XP ended 8/4/2014 so cannot be used to connect to NESCOT IT Facilities.
- Users are not permitted to save any personal or sensitive data from the college on their personal devices.
- You must not leave your computer or device unattended and unlocked whilst connected to any remote service.
- When using Wi-Fi, the user must ensure that the Wi-Fi is secure (requires a passcode to connect).

Please tick the box opposite to confirm you have read and understood Section 8 & 9	

- Users must ensure that the default passwords for routers and firewalls of the network you are connecting from has been changed from the default and that best security practices are being used.
- Users must refrain from using public Wi-Fi with no security e.g., coffee shops to connect to NESCOT services.
- All users must use adhere to all application security protocols and use Multi Factor Authentication where provided.
- Remote access services are only available to approved users.

10. Sanctions

- I understand that failure to comply with this Policy may lead to disciplinary action.

Please tick the box opposite to confirm you have read and understood Section 10	

Agreement

I have read and understand the rules and I agree to abide by them. If anything I do leads to legal action being brought against the College, I agree to accept responsibility.

Name (In Block Capitals):

Course:

Student ID Number:

By signing in the space below, I confirm that I have read and understood sections, 1-9

Signature:

Date: