Student IT Acceptable Usage Policy

Version 2

This policy applies to all NCLT institutions.

CONTENTS

1.0 Acceptable Use Policy

By using the Trust IT services in any of its school/colleges, you are agreeing to and are bound by the terms set out in this document and agree that all Trust devices and systems can be monitored for security and safety reasons, the Trust will not be responsible for any loss of data as a result of the system or students mistakes in using the system. Use of any information obtained via the network is at the student's own risk.

1.1 I agree that I will:

- Be responsible for my ICT activity and so will not give my username and password to anybody else and not attempt to log on using another person's username and password or access another person's files.
- Not attempt to gain unauthorised access to any part of the Trust network that is not available from my personal logon, either via the network or the Internet.
- Not connect any personal equipment to the Trust network without prior consent of the IT Manager.
- Not attempt to use or load programs, files, tools or shortcuts to gain access to either the hard drive of the Trust workstations or any other part of the network and not attempt to store any computer software on the Trust network.
- Not attempt to store any computer software on the Trust network that the Trust has no license for.
- Not attempt to store any free software on the Trust network without prior consent of the IT Manager.
- Immediately report any instance where I have inadvertently gained access to restricted areas to a member of staff.
- Only visit websites, which are appropriate to my work at the time and only use the Internet to help me with my work when using a Trust computer.
- Not visit websites that contain unsuitable material. If I am unsure if a site is suitable, I will ask a member of staff.
- Be responsible when setting a new password, minimum of 10 characters, include the following uppercase characters (A through to Z) lowercase (a through to z) Numbers (0 through 9), Special characters (example _, -, =, + ,!, @, *, /,)
- Not open unknown links and files in the interest of security/cyber-attacks.
- Save my work and log off properly after I have finished with the computer
- Not access or create any material that may cause upset to others.
- Ask IT support If I am unsure about opening or downloading any attachments or contents of an email.
- Not use portable media (like memory sticks) on the network without gaining permission from my teacher.
- Not attempt to set-up or use any proxy by-pass software, in order to by-pass the Trust Internet filter.
- Not meet anyone whom I have made contact with on the Internet without discussing this first with my parents/carers
- Not take information from the Internet and pass it off as my own work. If any work is found to have been plagiarised it will be given a Zero mark.
- Report any misuse of the Internet immediately to a member of staff.
- Be responsible in my use of email. I will not include in an email any material that is inappropriate. I will not use offensive or threatening language in my emails or in any other communication on the Internet. I understand that any email going out from the Trust will carry the Trust address and so represents the Trust.

- Always keep my personal details private.
- Only copy pictures or text into my area on the network. I will not download any other type of file, for example software, games, screen savers, Music, Films, etc.
- Use the Wireless or Guest Wireless network to the same responsible ways listed in this policy (depending which school or college site you are at)
- Not abuse the Printing and Copying services, all printing, copying and scanning is monitored and logged for abuse of use over and above normal practice.
- Not post any defamatory remarks relating to Trust Staff or Students to any Public Web sites either inside or outside the Trust, including Facebook, Twitter, Google +, and other websites where public users have access to view posts.
- Additionally, all Trust devices and systems can be monitored for security and safety reasons.
- All users accessing the bring your own devices wireless network do so under the agreement of Trust ICT Acceptable Use Policy and agree to adhere to conditions set out in this policy documentation. Students choosing to bring personal devices into the Trust do so at their own risk. (if applicable to your site)
- Treat Trust IT equipment with care and attention and accept that if I deliberately damage deface or vandalise IT equipment I will be charged the full cost and will be placed on contract, further action may be forthcoming in accordance with the behaviour policy of the school/college.

1.2 I accept that:

- The IT systems are provided to allow me to perform my work, whilst the Trust provides a reasonable level of privacy.
- I accept that any usage of the Trusts IT systems remains the property of the Trust; this may be stored data, emails images etc.
- The Trust may monitor any aspects of its computer systems that are made available to any user and may also monitor intercept and/or record any communications made, including telephones email or internet communications. The Trust will ensure compliance in line with the Regulation of Investigatory Powers Act (RIPA) 2000, and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

2.0 Criminal Conduct/Radicalisation and Extremism Test

2.1 Criminal Conduct/Radicalisation and Extremism related to the use of the Internet or email are covered by law, and by Trust policy and are unacceptable. These will be regarded by the Trust as constituting misconduct and any student involved will be subject to disciplinary action up to expulsion. These include: terrorist activities, on-line stalking, grooming, internet luring, soliciting of children by computer, defamation, retention of offensive screen savers, fraud, software theft, damage to Trust systems, retention of other people's personal details/information, drug-related activities, or any other illegal activity. The Terrorism Act (2006) outlaws web posting of material that encourages or endorses terrorist acts, even terrorist acts carried out in the past. Sections of the Terrorism Act also create a risk of prosecution for those who transmit material of this nature, including transmitting this material electronically.

2.2 Again, visits to websites related to jihadism/other forms of terrorism/ downloading of material issued by Jihadis /other terrorist groups (even from open-access sites) may be subject to monitoring by the police.

2.3 In addition, Section 26 of the Counter-Terrorism and Security Act 2015 places a duty on the Trust to have, in the exercise of its functions, due regard to the need to prevent people from being drawn into terrorism. This means that the Trust will place an appropriate amount of weight on the need to prevent people being drawn into terrorism in the application of this policy.

3.0 Social Media Advice and Policy

3.1 Please refer to the Social Media Policy located on the Trust website which clearly outlines the disciplinary procedures for students who use social media inappropriately.

4.0 Data Protection

4.1 Please refer to the Trust Personal Data Breach Policy and Data Protection Policy.

5.0 Further updates to this policy

5.1 This policy may be updated or modified at any time should the college deem it necessary. Sections of the acceptable usage policy will be displayed on your computer and must be accepted from time to time before web usage is allowed. The college reserves the right to administer these rules in a fair and unbiased way, which may result in a student's access to either the internet or the college network being removed or other appropriate sanction being taken.