Code of Practice for the Acceptable Use of IT facilities 2016/2017

Introduction

As a student the college provides you with access to a range of IT equipment to support your learning, to help you develop your skills for the future, gain experience of industry standard software and become confident in the use of IT.

Terms of Use

These guidelines apply to all computers, mobile devices, software and data within the college; or belonging to the college but located elsewhere. It includes the use of Student Portal/Moodle. It covers remote access from outside of the college, regardless of which device is used to make the connection e.g. personal computer at home, mobile phone. These resources are provided on the understanding that they are not misused in a way that will interfere with, disrupt or prevent anyone from legitimately using college resources.

You may use your personal laptop or other mobile device to connect to the college wireless network but you must ensure that the appropriate anti-virus / anti-malware protection is installed.

Use of the IT facilities is subject to the provisions of the Data Protection Act 1998, Copyright, Designs and Patents Act 1988, Protection from Harassment Act 1997, Communications Act 2003, Malicious Communications Act 1988, Public Order Act 1986, Obscene Publications Act 1959 and 1964, Protection of Children Act 1978, Sexual Offences Act 2003,Sex Offences Act 2003 Memorandum of Understanding and the Computer Misuse Act 1990, Counter Terrorism and Security Act 2015 and the Prevent Duty 2015.

What you may use college systems for:

College systems are provided for purposes related to your college course only. For any other use you will need to ask permission from your tutor or supervisor. You will be allocated a personal login after completion of all enrolment procedures.

- **Use of the Internet**

  Use of the Internet should be for research and finding sites that help in the completion of college work. Any sites that require payment for services should not be accessed. Should unsuitable sites be accessed inadvertently, please inform the appropriate member of staff.

- **Social Networking sites**

  Social networking sites e.g. Facebook are available on the majority of PCs in college unless a tutor has specifically asked for them to be blocked. There are also PCs in the Learning Resource Centres on which students can access social networking sites. We strongly advise students to set your privacy settings within these sites to ensure that only your friends/family can access what you post.

Please Note: when using such sites do not share your details with anyone you do not know.

What you may NOT use College systems for:

Creating, copying, sending, storing, displaying or receiving of:

- Any offensive, obscene or indecent images, data or other material
- Any material promoting terrorism or extremism.
- Material which is designed or likely to cause upset, annoyance, inconvenience or needless anxiety.
- Material which could be considered menacing, discriminatory, harassing, bullying, fraudulent or confidential/private
- Material that is for ‘leisure activity’ (e.g. playing games) unless this is an integral part of the course
- Material that infringes the copyright of another person, including unlicensed or illegal software

You must not create, run, send, store or transmit:

- Defamatory or libellous material
- Unsolicited commercial or advertising material
- Inappropriate material to any other network users or distribution lists that wastes network resources
- Personal resources e.g. photographs, music

You must not:

- Use other people's passwords or log in identities
- Change, copy, corrupt or destroy any other users' data
- Deliberately introduce 'viruses', 'worms', 'Trojans' or other harmful or nuisance programmes or files on to College systems
- Enable access to any non West Nottinghamshire College members without permission
- Install, remove or copy software
- Change screen savers or workstation configurations
- Disconnect cables on equipment or connect other devices to any PC

The college reserves the right to define all terms (e.g. 'offensive', 'menacing', 'indecent', 'defamatory' and 'libellous') in light of current legal and best industry practice standards.

Please Note: it is ILLEGAL to view indecent images of children – therefore, do not open any file that you suspect may contain such images. If you do receive suspicious files report it to your tutor.

Monitoring and Restrictions

The college has systems in place that monitor all Internet activity for breaches in the areas outlined above. If there is any reasonable belief that any of the regulations in this document are being broken (or criminal activities being undertaken), then these will be brought to the attention of college staff. Internet usage will be proactively monitored to detect and block any material promoting terrorism, violent extremism or which may be used to radicalise our staff and student body. The college may order the examination of Internet activity, email messages or network account data, in line with legal guidelines and in certain circumstances the police could be contacted. Internet traffic across personal devices connected to the college internet will also be monitored.

For security and legal purposes the IT team can access all data generated when users access/use IT systems, and any attempt to engage in activities with the aim of bypassing security or monitoring procedures (e.g. proxies) will be considered in breach of this agreement.

Disciplinary Action

If you contravene this or any policy related to the use of College IT systems, disciplinary action may be taken.