wqe | Wyggeston & Queen Elizabeth I College

IT Acceptable Use Policy

The college is committed to the equality of opportunity and to a proactive approach to equality, which supports and encourages under-represented groups, promotes inclusivity and values diversity

Policy Statement

The college seeks to promote and facilitate the proper and extensive use of IT and whilst the freedom of students, staff and other end-users of college IT systems is fully respected, this also requires responsible and legal use of the IT resources made available.

This Acceptable Use Policy is intended to provide a framework for such use of IT resources. The guidelines apply to all computing, telecommunication and networking facilities provided at the college and any new and developing technologies and uses not explicitly referred to.

College IT resources are provided primarily to facilitate a person's essential work as a student, employee or other role within the college. No use of any IT service should interfere with another person's studies or duties or any other person's use of IT, nor bring the college into disrepute in any way.

You may use your personal smart-phone, tablet, laptop, or other device to connect to the college wireless network in accordance with the Bring Your Own Device Policy.

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

Legislation

Users of the College's facilities are bound by UK laws. The following is an illustrative list of applicable UK laws, the Data Protection Act 1998, the Copyright, Designs and Patents Act 1988, the Protection from Harassment Act 1997, the Communication Act 2003, the Malicious Communications Act 1988, the Public Order Act 1986, the Obscene Publications Act 1959 and 1964, the Protection of Children Act 1978, the Sexual Offences Act 2003, the Computer Misuse Act 1990, the Counter Terrorism and Security Act 2015

Use of the Internet and Social Media

- The college is connected to the Joint Academic Network (JANET) and therefore this Acceptable Use Policy is taken to include the JANET Acceptable Use Policy and the JANET Security Policy as published by JANET (UK).
- Social networking sites are available on the majority of our computers unless they have specifically been blocked. Users must follow these social networking guidelines:
    - only make comments that you would also be prepared to make to someone directly
    - do not make comments that will bring you or the College into disrepute or damage your own or the Colleges reputation
    - remember that sites can be public and therefore accessible to anyone and to take extra care with these kinds of sites in terms of images or content
    - in social media, no matter your privacy settings, you are accountable for everything that you do and everything is public

PTO

- you are recommended to avoid storing your social media credentials on mobile devices in case of loss or theft. Always protect mobile devises with pin or biometric locks.

Users must not…

- use college computer systems to create, copy, send, store, display or receive:
  - any offensive, obscene or indecent images, data or other material
  - any material promoting terrorism or radicalisation
  - material intended or likely to cause upset, annoyance, inconvenience or needless anxiety
  - material which can be considered menacing, discriminatory, harassing, bullying or fraudulent
  - material which can be considered defamatory or libellous
- create or store an excessive amount of personal resources e.g. photographs, music, video unless required to do so for college activities
- disclose to others their username and password, or access, or attempt to access, computer systems for which permission has not expressly been granted
- leave unattended a computer that they are logged onto if in a classroom or other public place
- students should not disconnect cables; staff should reconnect them

You agree…

- there is no expectation of privacy when using college computer systems. Senior members of the IT team are able to access all data and materials
- the College, in meeting its duty under the Counter Terrorism and Security Act 2015, will proactively monitor the College's internet connection in order to detect any material promoting terrorism or radicalisation
- whilst the college takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of users files stored on college computer systems, it cannot, and does not give any guarantees about security, confidentiality, or integrity of your files
- contravening this or any policy related to the use of college IT systems that disciplinary action may be taken
- that using the College's IT systems and services means agreement with the Acceptable Use Policy and related policies