Information Technology and Email Usage Policy

Contact: Peter Liver, Chief Operations Director, Safeguarding and Prevent Lead for the College
Tel: 07494270799
Email: pliver@collegalpractice.com

Introduction and Scope

1.1 This policy applies to anyone using the College of Legal Practice’s information technology (IT) facilities. The information technology facilities include (and are not limited to) any hardware such as laptops, College issued mobile phones, all software, network access and online services such as email and internet usage.

1.2 This policy applies to all employees of the College and all students. In addition, visitors to the College and any external partners who access the College's online services are also required to adhere to this policy.

1.3 On occasions, IT facilities are provided primarily to facilitate a person’s essential work as an employee or student or other role within the College. Any IT facilities provided to individuals will remain the property of the College and should be used to further the work of the College.

1.4 Users of IT facilities are reminded that they remain subject to the same laws and regulations as in the physical world and, as such, it is expected that all conduct on our systems is lawful. Furthermore, where services are accessed from outside of the United Kingdom, users are reminded that they are also required to abide with local laws and regulations.

1.5 Breach of any applicable law or third-party regulation/requirements will be regarded as a breach of this policy. This includes the terms of any software licences procured by the College which are brought to your attention.

1.6 The College reserves the right to monitor and block access to indecent, offensive, threatening or discriminatory or extremist material.

Responsibility

2.1 The Chief Operations Director (or nominee) has the responsibility for interpreting and enforcing this policy.

2.2 All users of the IT facilities must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of this policy. Any queries about these instructions should be directed to the Chief Operations Director (or nominee).

Personal Use of College IT Facilities

3.1 Any IT facilities provided by the College may be used for reasonable personal use. This is provided that this personal use does not infringe any requirements of this policy and does not interfere with the valid College activity related use of the facilities by other users.

3.2 The College reserves the right to remove access to its IT facilities for personal use at any point.

3.3 The IT facilities should not be used to advertise any trade, service or profession not endorsed by the College. Any queries about whether a commercial activity may be undertaken using the IT facilities should be directed to the Chief Operations Director or nominee before commencing the relevant use of the IT facilities.

3.4 The College's IT facilities must not be used to plagiarise the work of others or to facilitate an act which may lead to an allegation of academic misconduct.

Identification and Access

4.1 It is the responsibility of all users to take reasonable precautions to safeguard any IT credentials (for example a username and password or email address).

4.2 Users must not share their IT credentials with other individuals. No one in the College has the right to ask a user for a password. In addition, users must not attempt to obtain or use anyone else's IT credentials.

4.3 Users must not impersonate someone else or disguise their identity when using the IT facilities.

4.4 Administrative access to any IT facility can only be provided by the Chief Operations Director (or nominee) and it is expected that there should be sufficient justification that the role of the individual requires such access. Where administrative access is granted, a user may need to agree to additional conditions to this usage and level of access.

IT Infrastructure

5.1 Users must not do anything to harm the integrity of the IT infrastructure by, for example, doing any of the following without approval:

5.1.1. Damaging, deleting, reconfiguring, moving or removing equipment

5.1.2. Loading software on to IT equipment other than in approved circumstances

5.1.3. Reconfiguring or connecting equipment to the network other than by approved methods

5.1.4. Setting up servers or services on the network

5.1.5. Deliberately or recklessly introducing malware

5.1.6. Attempting to disrupt or circumvent IT security measures

Handling Personal, Confidential or Sensitive Information

6.1 Where users handle personal, confidential or sensitive information, they must take all reasonable steps to safeguard it and observe the College's privacy and data protection policies. Users should also be particularly mindful of this when using their own mobile or IT devices.

6.2 Users must ensure they do not engage in the following activities:

6.2.1. Infringing copyright or breaking the terms of licences for software or other material.

6.2.2. Accessing, deleting, modifying or disclosing information which belongs to another without their permission or without the agreement of the Chief Operations Director.

6.2.3. Creating, downloading, storing or transmitting unlawful material, or material that is indecent, offensive, threatening or discriminatory or extremist.

Online Behaviour

7.1 Users are reminded that real world standards of behaviour apply online and on social media/networking platforms.

7.2 The following actions are expressly forbidden by this policy:

7.2.1. Causing needless offence, concern or annoyance to others.

7.2.2. Sending spam (unsolicited bulk email).

7.2.3. Deliberately or recklessly consuming excessive IT resources such as processing power, bandwidth or consumables.

7.2.4. Using the IT facilities in a way that interferes with others' valid use of them.

7.2.5. Inappropriate use of social media platforms, which presents the College in a negative or derogatory manner.

7.2.6. Accessing details of other employees or students for personal reasons or for reasons outside of College purposes.

7.2.7. Viewing illegal or obscene sites and/or material or sites which may be a source for viruses

7.3 As set out in the College's Prevent Policy, the College has a duty to take steps to prevent people from being drawn into terrorism. The College also has a duty to provide staff and students with an environment where freedom of expression and speech (within the law) are protected but balanced with the need to ensure that the College is free from harm and hatred. Given the nature of the curriculum at the College, we would not expect any members of staff or students to have a need to legitimately access extremism related or terrorist related content on the College IT infrastructure. This includes the creation, download, storage, transmission or display of material that promotes or incites racial or religious hatred, terrorist activities or hate crime; or instructional information about any illegal activities. As such, access to such materials is prohibited.

7.4. Where a member of the College's staff or student base considers they have a legitimate need to access such material on the College's IT system, they should discuss this need with their Personal Tutor or Supervisor (if a student) or with the Prevent Lead, Chief Operations Director to first seek permission.

7.5. Given the size of the College and given that student do not access online materials on the College's IT infrastructure (for example, through the provision of IT equipment and access to the College network or a shared Wi-Fi), the College has not considered it proportionate to implementing filtering at this time. However, the College is working with the Counter Terrorism Internet Unit Internet Referral Unit to block access to the CTIRU complies list of URLs. This position will be kept under review with the Prevent Lead and the College reserves the right to introduce filtering in the future.

Monitoring

8.1 The College reserves the right to monitor and record the use of its IT facilities, including email, internet and other communications for the purposes of:

8.1.1. The effective and efficient planning of operation of the IT facilities.

8.1.2. Detection and prevention of infringement of this policy.

8.1.3. Investigation of alleged misconduct.

8.1.4. To protect the IT facilities against viruses and hackers.

8.1.5. To assist in the investigation of breaches of this policy.

8.1.6. To prevent or detect suspected or possible misconduct or crime or other unauthorised use of the IT Facilities.

8.1.7. To comply with any legal obligation.

8.2 The College may also access or monitor IT facilities to pursue the College's other legitimate interests, such as the detection of an act which could amount to an academic misconduct, or by accessing files and reviewing the emails of employees who are absent, or to enable the office functions to be undertaken/shared by appropriate members of staff.

8.3 Where monitoring or access is carried out by the College it will be undertaken in accordance with all applicable legislation relating to data protection and employee monitoring. Any monitoring / access will only be carried out with the consent of the Chief Operations Director.

8.4 The College will also comply with all lawful requests for information from government and law enforcement agencies.

8.5 Emails may need to be used in legal proceedings and even emails which have been deleted may remain in Archive systems and are capable of being retrieved.

Infringement

9.1.The College may take action in accordance with the College's relevant disciplinary procedures where a user breaches the provisions of this policy.

9.2.The College reserves the right to suspend a user's access to specific IT facilities where an investigation into an alleged breach of this policy is being carried out and, in its discretion, permanently to withdraw access where a breach is established.

9.3.The College will cooperate fully with any police investigations in relation to the use of IT facilities and this may include the College reporting unlawful activities to the relevant law enforcement agencies.

9.4.Where derogatory or damaging material is posted online, the College may pursue an action requiring this information to be taken down. The College reserves the right to recover any costs incurred by the College as a result of a user's infringement of this policy.