The Inns of Court College of Advocacy

Acceptable IT Usage Policy for ICCA Students

Version 1.0

I. Purpose & Scope

The ICCA provides IT services primarily for academic and operational purposes to support learning and teaching. IT services must be used responsibly, in accordance with the law and ICCA policies in ways that do not bring the ICCA into disrepute. This policy stipulates the practices and constraints that apply when accessing and using the ICCA's IT services.

This policy applies to all students who access the ICCA's IT services on ICCA owned and personally owned devices.

This policy provides overarching direction for IT services and resources provided to ICCA students. There are other related policies and specific subsidiary procedures covering a range of IT user activities and aligned with this policy that must also be followed.

II. Definitions

An IT service is one based on the use of information technology and supports the institution's academic and business processes. At the ICCA, IT service is made up of a combination of people, processes and technology. IT services provided under contract are defined as services provided by a third-party organisation outside of the university.

ICCA system – any system or application which supports the ICCA's academic and business processes.

Personal data – any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier (e.g. name, identification number, location data or online identifier).

Special category personal data – the following types of personal data (specified in data protection legislation) which are particularly sensitive and private in nature, and therefore more likely to cause distress and damage if compromised: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health related conditions (physical or mental health), sex life and sexual orientation, commission or alleged commission of any criminal offence, genetic data, biometric data, where processed to uniquely identify an individual.

Auto-forwarding/Redirecting email – this is the capability of automatically forwarding incoming email messages from one user account to another user account.

A mobile device is a portable computing device (e.g. smart phone, tablet, laptop, portable storage device).

Information security refers to the procedures, processes and guidance which are designed and implemented to protect COIC or ICCA information from unauthorised access, use, misuse, disclosure, destruction, modification or disruption.

Physical and environmental security is the protection of personnel, premises, facilities, hardware, software, networks and data from physical actions and events that could cause serious

loss or damage to the university. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism.

III. Policy

1. Introduction

1.1 IT services are provided by the ICCA for academic and business purposes. Acceptable use of IT services must be lawful, reasonable and raise no unnecessary risks or security threats for the ICCA.

1.2 In particular, the ICCA has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The ICCA reserves the right to block or monitor access to such material.

1.3 All IT resources provided are the property of the ICCA and must be used or accessed in accordance with this policy and its related procedures.

2. ICCA Credentials: Username and Password

2.1 Users must take all reasonable precautions to safeguard their usernames, passwords and any other IT credentials issued to them. They must not allow anyone else to use their IT credentials.

2.2 Users will be held responsible for all activities undertaken using their credentials.

2.3 Users must not attempt to obtain or use anyone else's credentials.

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

2.5 Passwords must conform to guidance regarding length and complexity established by IT from time to time.

2.6 Passwords must be unique to the system being accessed and not used to access any other system.

3. Confidentiality

3.1 Individuals who handle personal, confidential or sensitive information must take all reasonable steps to safeguard it and must be aware of and observe the requirements of the ICCA's Data Protection Policy.

3.2 Any breaches of confidence relating to confidential information held by the ICCA may be treated as a disciplinary offence (under student disciplinary procedures) and may constitute an offence under data protection legislation or regulation.

3.3 Users must ensure that any data exported from ICCA systems is handled in such a way as to maintain the confidentiality and security of that data.

4. Accessing and Using ICCA Systems

4.1 Any access or attempt to access ICCA systems and information for which permission has not been granted will be treated as a disciplinary offence.

5. Email

5.1 This policy covers the use of ICCA email accounts assigned to individuals or groups. It also applies to other collaborative tools, such as Microsoft Teams, Microsoft Groups and shared mailboxes where these tools make use of the ICCA's email service.

5.2 ICCA email accounts must be used to conduct ICCA business.

5.3. Emails sent, received or generated from an ICCA email account in the course of all ICCA business, academic and administrative, are the property of the ICCA.

5.4. Assigned ICCA email addresses are for the sole use of the individual user. Access to a user's mailbox without the user's permission is prohibited, unless an exception has been approved under the Email Procedures.

5.5. The use of email must in all ways meet the conditions of the ICCA's policies concerning communications: dignity, equality, diversity, inclusion and respect.

5.6. Email users must take reasonable measures to prevent the transmission of viruses, such as not opening email attachments received from unsolicited sources.

6. Information Security

6.1 Information security measures protect information from a wide range of threats and safeguard information. The ICCA's information security measures are based on the following principles:

- **Confidentiality** to ensure ICCA information is not made available or disclosed to people or organisations who do not have authorisation to see it.
- **Integrity** to ensure that ICCA information is complete and error-free.
- **Availability** to ensure that ICCA information and associated services are available to authorised users when required.

6.2 The ICCA will:

- Maintain a secure environment in which to create, use and store information.
- Protect all confidential, restricted and personal/sensitive personal information from unauthorised use and disclosure.
- Comply with regulations and laws to avoid any penalties or fines for non-compliance.

6.3 All users of the systems must immediately report any suspected breaches, cyber attacks or security related issues via the IT help Desk. in the case of a breach that may compromise personal data, must also notify the Director of operations team immediately. Select this link to view the guidance for reporting a breach.

7. Unacceptable Use

7.1 The following are examples of unacceptable use. The list is not exhaustive.

- Creating, transmitting, storing or displaying insulting, indecent or obscene material.
- Creating, transmitting, or displaying material that deliberately and unlawfully discriminates, or encourages deliberate and unlawful discrimination, on the grounds of race, ethnicity, gender, sexual orientation, marital status, age, and disability, political or religious beliefs.
- Creating, transmitting, or displaying material that encourages terrorism and/or invites support for a proscribed terrorist organisation.
- Creating, transmitting or displaying defamatory material.
- Obtaining, transmitting or storing material where this would breach the intellectual property rights of another party. This includes downloading and sharing music, video and image files without proper authority.
- Contravening the policy of a third-party company with which the university holds a contract for IT services.
- Creating or transmitting material with the intent to defraud.
- Creating or transmitting material or using ICCA systems for commercial purposes unrelated to the interests of the university.
- Causing annoyance or inconvenience, e.g. sending unsolicited email chain letters, unauthorised bulk email (spam), which is unrelated to the legitimate business of the university.
- Sharing information when not authorised to do so (especially commercially sensitive, personal and sensitive personal data).

- Intentionally interfering with the normal operation of the network, including the spreading of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.

8. Monitoring and IT Access

8.1 The ICCA monitors and records the use of its IT facilities for various purposes including:

- The effective and efficient planning and operation of IT facilities.
- Detection and prevention of infringement of this policy, related procedures and relevant legislation.
- Investigation of alleged misconduct.
- Compliance with lawful requests for information from government and law enforcement agencies.

8.2 Where personal data is being processes as part of these activities, the GDPR lawful basis is that such monitoring is necessary for the ICCA's legitimate interests, and these interests override the impacts on the users.

8.3 The Dean of the ICCA, may authorise access to a user's accounts for any of the reasons noted in 8.1 or to permit ongoing ICCA operations in the event of the death, incapacity, suspension, dismissal, departure or long-term absence of a user.

8.4 Before authorisation is granted, a Data Protection Impact Assessment must be carried out to identify the purpose of the access, the adverse impact on individuals, whether there are less intrusive means of achieving the aim, and whether the access is justified.

9. Enforcement

9.1 Following the requirements of this policy, other associated policies and procedures will ensure that users comply with the law. However, users should contact the IT Service Desk for advice about any concerns.

9.2 Non-compliance with this policy or associated procedures is an infringement of the ICCA's regulations and will be investigated in accordance with the ICCA Academic Regulations.

9.3 The ICCA may remove or limit a user's access to the ICCA's systems on a temporary basis when that is deemed necessary to protect the system or prevent reputational damage to the ICCA or in the course of an investigation.

9.4 On the recommendation of the ICCA Dean, further access limitations or permanent denial of access may be imposed by the ICCA.

10. Review

10.1 This policy shall be reviewed at least every three years.