COURAGE CONSULTANTS UK LIMITED

ICT (Information Computing Technology) Policy

Version 1.3
Date Created 01/07/2021
Most Recent Review Date 02/05/2023
Next Review Date 02/05/2024

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

COURAGE CONSULTANTS UK LIMITED

Version Control

Document Title	Courage Consultants UK Limited ICT (Information Computing Technology) Policy
Version	Version 1.0.
Approved by	Omoruyi Courage Ogbewe
Policy Lead	Omoruyi Courage Ogbewe
Date of Original Approval	20/09/2023
Date of Last Review	20/09/2023
Changes made at the last review	Document Creation
Date effective from	20/09/2023
Date of next review	20/09/2024

Contents

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

COURAGE CONSULTANTS UK LIMITED

1. Policy Statement

1.1. Courage Consultants UK Limited recognises the vital role information technology plays in Courage Consultants UK Limited missions and related administrative activities as well as the importance in an academic environment of protecting information in all forms.

1.2. As more information is used and shared in a digital format by students and staff, both within and outside Courage Consultants UK Limited, an increased effort must be made to protect the information and the technology resources that support it.

1.3. Increased protection of our information and Information Technology Resources to assure the usability and availability of those resources is the primary purpose of this Policy.

1.4. The Policy also addresses code of practice for the use of IT facilities at Courage Consultants UK Limited.

2. Purpose

2.1. The purpose of this policy is to inform Courage Consultants UK Limited staff, students, visitors, and other stakeholders the use of information computing technology facilities owned and provided by Courage Consultants UK Limited.

2.2. This policy concerns all computer systems, networks and Wi-Fi facilities operated by Courage Consultants UK Limited at all its campuses and regardless of location, where responsibility for user management and control resides with members of staff of Courage Consultants UK Limited, or where it may be outsourced to third parties.

2.3. This policy has been developed to help ensure that Courage Consultants UK Limited information computing technology, in its widest sense, is protected against unauthorised use and unauthorised access. In particular, the policy has been developed to help ensure protection against unauthorised access and modification to Courage Consultants UK Limited' various data systems and other ICT systems.

3. Scope

3.1. This policy applies to:

- All full-time, part-time, and temporary staff employed by, or working for or on behalf of Courage Consultants UK Limited
- All students studying at Courage Consultants UK Limited
- Contractors and consultants working for Courage Consultants UK Limited
- All other individuals or groups, including visitors, who have been granted access to Courage Consultants UK Limited ICT facilities.

3.2. It is the responsibility of each person to whom this policy applies to fully adhere to its requirements. This policy concerns:

- The use of Courage Consultants UK Limited owned ICT facilities, including information systems.
- Courage Consultants UK Limited network facilities (wired and wireless) regardless of whether these are used through the connection of Courage Consultants UK Limited

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

owned equipment or through the connection of private equipment to Courage Consultants UK Limited owned equipment.

4. Code of Practice

4.1. Conditions of Use

4.1.1. Individuals may use Courage Consultants UK Limited ICT and Wi-Fi facilities if authorised to do so and are:

- An employee of Courage Consultants UK Limited
- A student registered for a programme of study at Courage Consultants UK Limited /our partners
- A former member of staff
- An individual or a member of a group who has been permitted to use Courage Consultants UK Limited ICT
- A visitor to Courage Consultants UK Limited

4.2. Only the Chief Executive Officer or Managing Director may authorise individuals or groups to use and access Courage Consultants UK Limited facilities.

4.3. Courage Consultants UK Limited ICT facilities must not generally be used for, or in connection with, the activities identified below, some of which could result in legal action or civil proceedings being mounted against either an individual, Courage Consultants UK Limited, or both:

a) Deliberately accessing, creating, or transmitting any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, with the exception of data which is connected with Courage Consultants UK Limited work or official research or other professional activity, where the sender/recipient would expect to exchange such material with other users in a professional capacity.
b) Creating, transmitting, or accessing material which is designed or likely to cause offence, annoyance, inconvenience, or needless anxiety to another.
c) Creating, transmitting, or accessing material which runs the risk of drawing people in to, or towards, terrorism and/or extremism, except where it can be demonstrated that there is a legitimate academic interest.
d) Deliberately contributing to News Groups or web sites that advocate illegal activity.
e) Creating or transmitting defamatory material or material that is libelous of any other person's or company's reputation, products, or services.
f) Viewing, transmitting, copying, downloading, or producing material, including (but not exhaustively) software, films, television programmes, music, electronic documents, and books which infringes the copyright of another person, or organisation.
g) Making offensive or derogatory remarks about staff, students or Courage Consultants UK Limited on interactive social and life-style websites such as Instagram, Facebook, and Twitter.

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

h) Posting offensive, obscene, or derogatory photographs, images, commentary, or soundtracks on interactive social and life-style websites such as Facebook, Twitter, and YouTube.
i) Transmitting or producing material which breaches confidentiality undertakings.
j) Attempting to gain deliberate access to facilities or services which you are unauthorised to access.
k) Deliberately undertaking activities that corrupt or destroy other users' data; disrupt the work of other users or deny network resources to them; violate the privacy of other users; waste staff effort or networked resources.
l) Creating or transmitting unsolicited commercial or advertising material unless that material is part of a service to which recipients have chosen to subscribe.
m) Making commitments via email or the Internet on behalf of Courage Consultants UK Limited without full authority.
n) Undertaking any activities detrimental to the reputation or business interests of Courage Consultants UK Limited.
o) Initiating or participating in the sending of chain letters, 'junk mail', 'spamming' or other similar mailings.

4.4. Any user who inadvertently accesses an inappropriate Internet site must immediately close the session or return to the previous page.

4.5. Any member of staff who receives an inappropriate email message or e-mail content that appears to have been sent by a member of staff or student may wish to report the matter to the Chief Executive Officer or Managing Director.

4.6. Use of Private Equipment

4.6.1. Privately owned equipment of staff, students and other individuals or groups may only be connected to Courage Consultants UK Limited Wi-Fi upon agreement of either the Chief Executive Officer or Managing Director. Courage Consultants UK Limited accepts no responsibility for the effects that any such connection may have on the operability of privately owned electronic or other devices, consequently all risks, however small, reside with the owner.

5. Legal Obligations

5.1. All use of Courage Consultants UK Limited ICT facilities must be in full compliance with the law, and where appropriate, all other regulations which are applicable.

5.2. All individuals must not try to gain unauthorised access to any computer system anywhere at Courage Consultants UK Limited. This is commonly known as hacking and constitutes a criminal offence under The Computer Misuse Act 1990. In certain cases, such activities can also be contrary to other legislation, for example, The Terrorism Act 2000.

5.3. All individuals who have access to Courage Consultants UK Limited systems must not do anything maliciously, negligently, or recklessly which might cause any sort of harm or disruption to any computer system anywhere (worldwide), or to any of the programs or data on any system. In this context the word harm is taken to mean any kind of damage, and any kind of unauthorised access, denial of resources or any data alteration.

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

5.3. If users are reasonably requested to do so, you must justify your use of Courage Consultants UK Limited ICT facilities and/or Wi-Fi facilities. You must explain (in confidence, if necessary) what you are doing, and how and why you are doing it. You must make any reasonable changes requested by senior staff and comply with any reasonable restrictions placed upon you.

5.4. All users must comply with valid regulations covering the use of software and datasets, whether those regulations are made by law, by the producer or supplier of the software or datasets, by Courage Consultants UK Limited, or by any other legitimate authority. Where you have any doubts, you must contact the Chief Executive Officer or Managing Director before using Courage Consultants UK Limited ICT facilities.

5.5. Whilst every reasonable endeavor is made to ensure that the ICT facilities and Wi-Fi facilities are available as publicised and scheduled and function correctly, no liability whatsoever can be accepted by Courage Consultants UK Limited for any direct or consequential losses or delays as a result of any system malfunction.

6. Computer Crime and Misuse

6.1. Courage Consultants UK Limited expects users to use ICT facilities, and in particular email and the Internet, responsibly at all times. Suspected computer crime and misuse of Courage Consultants UK Limited ICT facilities, including excessive personal use by staff, will be investigated by the Managing Director and action taken accordingly.

7. Monitoring use of Courage Consultants UK Limited ICT Facilities

7.1. Under the Telecommunications (Lawful Business Practice [LBP]) (Interception of Communications) Regulations 2000 (Statutory Instrument 2000 No.2699) Courage Consultants UK Limited reserves the rights to monitor users' activities to:

- Record evidence of official transactions
- Ensure compliance with regulatory or self-regulatory guidelines (including this Policy)
- Maintain effective operations of systems (for example, preventing viruses)
- Prevent or detecting criminal activity
- Prevent the unauthorised use of computer and telephone systems to ensure that the users do not breach Courage Consultants UK Limited policies.

7.2. Under this regulation there is a requirement for employers to inform staff about such monitoring. The publishing of this Policy is one means of fulfilling that obligation.

8. Policy Review

8.1. This policy may be amended by Courage Consultants UK Limited at any time and will be reviewed annually to ensure it is fit for purpose. Any issues related to the monitoring and review of this policy, please contact courage@courageconsultants.co.uk

9. Data Protection and Confidentiality

9.1. Courage Consultants UK Limited is registered with the Information Commissioner's Office as a Data Controller. Details of the School's registration are published on the Information

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP

Commissioners website. Courage Consultants UK Limited as a Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the UK General Data Protection Regulations (UK GDPR) and under the Data Protection Act 2018 (DPA).

9.2. The UK GDPR and DPA regulates the use and storage of personal information (i.e., any information which identifies a living individual) on computing systems. It is the user's responsibility to ensure that their information and computer usage complies with this law. Failure to do so could result in criminal charges being brought against both you and Courage Consultants UK Limited.

10. Alternative Format

10.1. This policy can be provided in alternative formats (including large print, audio and electronic) upon request. For further information, or to make a request, please contact: courage@courageconsultants.co.uk

Courage Consultants UK Limited,
Unit 122 Riverpark business Centre, Riverpark Road
Manchester, M40 2XP