CCL
Corndel College London

IT Acceptable Use Policy

A. Purpose

1. This policy outlines the acceptable use of IT resources provided by Corndel College London to ensure a safe, secure, and respectful digital environment that supports academic excellence, personal development, and institutional integrity.

B. Context and Scope

2. The Institution operates entirely in the cloud and does not manage its own servers or networks. As a fully remote organisation, all access to systems is internet-based and all IT services are delivered through vetted Software-as-a-Service (SaaS) platforms, which are regularly reviewed for cybersecurity and data protection compliance.

3. Access to platforms hosting personal data is secured using Multi-Factor Authentication (MFA), and where possible, Single Sign-On (SSO) via Office 365 which requires MFA with geolocation and a two-digit confirmation code. Microsoft Defender for Office 365 tenant is provided to screen out junk, spam and phishing emails.

4. This policy applies to all staff and applies, as relevant, to students, contractors, and visitors who access or use the institution's IT systems, networks, devices, and/or data. The IT Acceptable Use is covered as part of staff and student inductions and onboarding processes.

C. User Groups and IT Access

- **Staff and Contractors**

5. Staff members are granted comprehensive access to the institution's IT systems, platforms, and data, as appropriate to their roles and responsibilities. This access is governed by role-based permissions and is subject to regular review to ensure it remains appropriate and secure. Staff are expected to use IT resources responsibly and in accordance with this IT Acceptable Use Policy, the Information Security Policy, and all relevant data protection and Safeguarding regulations. Any

misuse of IT systems may result in disciplinary action. Staff must also report any security incidents or breaches promptly to the IT department.

6. Contractors may be provided with access to IT systems based on the specific tasks or roles they are contracted to perform. This access may include a temporary institutional email address, limited use of Microsoft 365 applications, and secure access to designated files or systems. Contractors visiting the office may be granted access to Wi-Fi for the duration of their visit. All access is time-limited and will be revoked upon completion of the contract or project. Contractors are required to comply with this IT Acceptable Use Policy and any additional contractual or security requirements. Misuse or unauthorised access may result in termination of access and further action.

- **Students Studying on Degree Apprenticeship Programmes**

7. Corndel College London solely delivers its teaching online. Students studying a Degree Apprenticeship Programme, are provided with secure, limited-access accounts within Corndel's IT platforms and are provided with access to limited Microsoft Office apps, 365 accounts and an Institutional email address for educational purposes and for the duration of their learning.

8. Students are encouraged to and use IT equipment and environments provided by their employers. Corndel College London IT Acceptable Use Policy does not apply to employer-provided systems and software and students should comply with their employer's Acceptable IT Use, Data Protection, and Information Security policies.

9. Training on data protection and responsible IT use is included in the academic curriculum. Additional information and guidance can be found in Corndel College London's Ethic's Policy. To promote safe and lawful IT use, students studying Degree Apprenticeship Programmes are provided with the E-Safety Policy as part of their induction and onboarding. Students undertaking Apprenticeship Degree Programmes should also refer to their employer's E Safety Policy.

- **Visitors**

10. Visitors to the institution have minimal access to IT systems and would typically attend meetings online. When physically present on-site, they may be granted access to Wi-Fi and, where necessary, temporary access to specific files or

platforms for meetings or collaborative purposes. Visitors must use IT resources solely for the intended purpose of their visit and in a manner that is respectful and secure. Any misuse of IT systems by visitors may result in immediate revocation of access and notification to relevant authorities.

11. This policy should be read in conjunction with the following policies which can be found on the website at www.corndelcollege.com

- Information Security Policy
- E Safety Policy
- Ethic's Policy
- Freedom of Speech Code of Practice
- Safeguarding Policy
- Anti-Harassment and Bullying Procedures.
- External Speaker Procedure
- Equal Opportunity Policy

This is not an exhaustive list. CCL may consider other legislation, where relevant.

D. Legal and Ethical Compliance

- **Data Privacy and Protection**

12. The Institution upholds the highest standards of data protection and privacy in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. These laws establish the legal framework for the collection, use, storage, and transfer of personal data, ensuring that individuals' rights are respected and protected.

13. As appropriate to their user group set out in this policy, users have a legal and ethical duty to safeguard personal and sensitive data, particularly when transferring data across systems and networks. This includes ensuring that data is processed lawfully, transparently, and for legitimate purposes, and that appropriate technical and organisational measures are in place to prevent unauthorised access, loss, or misuse.

14. Personal data must be collected, stored, and processed lawfully, fairly, and transparently. In addition, sensitive data must be encrypted and shared only with

authorised individuals and in line with the relevant appropriate Data Privacy Policy.

15. Access Corndel's Data Protection Policy for more information. For support with Corndel's Data Protection Policy, please contact gdpr@corndel.com.

16. Please note that students undertaking Degree Apprenticeships must also comply with their employer's Data Protection Policy and should refer to their employer for further details.

- **Academic Freedom and Freedom of Speech**

17. Freedom of speech and academic freedom are foundational principles of higher education delivery. These principles support the open exchange of ideas, critical thinking, and the pursuit of knowledge. They give freedoms which allow users of this policy to express lawful views, even if controversial or unpopular and without fear of censorship or institutional correction based on undue influence or restriction arising from external pressures or internal policies.

18. Corndel College London complies with the Higher Education (Freedom of Speech) Act 2023, Education (No2) Act1986 and the Human Rights Act 1998. The Institution promotes academic freedom and lawful freedom of speech and expects users to express views and engage in debate, provided it does not incite violence, hatred, harass or discriminate under the law. Speech that constitutes unlawful acts is not protected by law and Corndel College London takes seriously its duty to balance the protection of these freedoms with its other duties under the Equality, Safeguarding, Counterterrorism and Data Protection laws.

19. As such, content shared via institutional platforms must be respectful and aligned with institutional values and in compliance with law. For more information, please refer to the Freedom of Speech Code of Practice and the Event and Speaker Procedure.

- **Safeguarding (including Prevent Duty protection from harassment and sexual misconduct)**

20. The Institution is committed to Safeguarding (including Prevent and protection from harassment and sexual misconduct) and protect members of its community including students and staff from harm, abuse, neglect, and exploitation by:

i. Creating a safe learning environment;
ii. Having robust policies and procedures;
iii. Training and briefing staff and students;
iv. Identifying and promoting awareness of risks; and
v. Responding appropriately to concerns and providing appropriate support for staff and students

21. As such, under this policy:

i. Users must not access, create, store or distribute content that promotes extremism, radicalisation, or harm to others such as pornography or engaging in gambling.

ii. IT systems may be monitored to ensure compliance with safeguarding obligations.

22. Any concerns related to Safeguarding (including Prevent Duty protection for harassment and sexual misconduct) must be reported to the Designated Safeguarding Lead by sending an email to safeguarding@corndel.com. Please refer to the Safeguarding and Prevent Policy, for more information.

- **Equality, Diversity and Equality duty**

23. The Institution is committed to the Equality duty and promoting equality, eliminating discrimination, and fostering an inclusive environment for all users of its IT systems, regardless of their protected characteristics such as age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation. Users should ensure their digital content and communications are accessible, inclusive as well as considers the needs of users with disabilities. For more information, please refer to the Equal Opportunity Policy.

E. IT Acceptable Use Guidelines

- **General Use**

24. IT and other electronic resources (including company telephone/mobiles) must be used responsibly, ethically, and legally.

25. Users must not engage in activities that disrupt or compromise the integrity, security, or performance of IT systems. Such as downloading unacceptable

content or leaving laptops and company mobile phones unattended. Please see Appendix A for tips on **'Keeping your Device (Laptop and Mobile Phone) Safe and Secure'.**

26. Passwords for access to the system are confidential and must not be revealed to other persons. **Please also refer to paragraph 32, 'Passwords' below more information.**

27. The personal use of IT and electronic resources is permitted within reasonable limits, provided it does not interfere with institutional operations or breach this policy.

- **Security and Access**

28. Users must protect their login credentials and report any suspected breaches immediately. Any unauthorised access to systems, data, or accounts is strictly prohibited. For example:
    i. Copying of ANY data to external USB devices is banned and technologically enforced.
    ii. Playing games on the system, or individual computers is not permitted.

29. Devices must be kept secure and updated with institution-approved security software. All software must be authorised by the employee's Line Manager and approved by the institution's IT Department, before they are uploaded onto the Institution's computer.

30. All data must be stored in the users One Drive. Users SHOULD NOT save any file on their desktop under 'This PC.'

31. Upon the discovery of a computer virus and/or corrupted information, users must immediately contact the IT Support Desk by sending an email to itsupport@corndel.com

- **Passwords**

32. Passwords for access to the system are confidential and should never be given/shared with anyone. **It is recommended that passwords should:**
    i. contain at least 8 characters and include at least one number or special character such as #, €, % etc.

ii. be changed on a regular basis, ideally every 30 days.
iii. never be reused or contain 'guessable' information/data/words such as names, birthdays, addresses etc.
iv. never be written down or stored in any kind of input completion programme.

33. **E-mail and use of electronic communications app**

34. Institutional email accounts and other electronic communication apps such as Teams are provided to support academic, administrative, and operational activities. To ensure security, accountability, and professionalism all users must use their official email accounts and other electronic communication apps for institution-related communications. Users should:

    i. Ensure all communications are respectful, professional, and appropriate.

    ii. Avoid using offensive, obscene, or inflammatory language as prescribed by law.

    iii. Not sending bulk emails without prior authorisation.

    iv. Be cautious of phishing attempts and report suspicious emails immediately. Take care not to send unsolicited (spam/junk) emails. Microsoft Defender is enabled on Corndel's Office 365 tenant which screens out most junk, spam and phishing emails sent to any Corndel email address. However, particular attention should still be paid to phishing/junk emails and users should use the 'Report' button provided to send any suspected phishing emails to the IT Team.

    v. Avoid sending sensitive or personal data via email unless encrypted and authorised.

    vi. Regularly review and delete unnecessary emails to maintain system efficiency.

    vii. Not impersonate others or misrepresent your identity.

    viii. Avoid sending sensitive or personal data via email and other electronic communication unless encrypted and authorised.

35. For more information, please refer to the E Safety Policy.

F. Prohibited Activities

36. This policy does not permit:

    i. Accessing or distributing illegal, offensive, inappropriate, or confidential content.

    ii. Using IT resources for harassment, bullying, or discrimination as prescribed by law. For more information, please refer to the Anti-Harassment and Bullying Procedures.

    iii. Unauthorised copying or distribution of copyrighted materials.

    iv. Introducing malware or attempting to bypass security controls including downloading, opening and distributing unauthorised software.

G. Monitoring and Enhancement

37. The Institution ensures its business network is safe and secure and makes every effort to keep its security software up to date. The security measures include the use of enhanced filtering and protection of firewalls, servers, routers, laptops etc. to prevent accidental or malicious access of systems and information. The Institution reserves the right to monitor/audit internet and IT use including email and other communication apps, in accordance with institutional policies and legal requirements to ensure compliance. Users will be notified of monitoring practices and their rights under applicable policy and law, as necessary.

38. Breaches of this policy may result in disciplinary action, including suspension of access, academic sanctions, or legal referral. For more information, please refer to the Staff Disciplinary Policy. For more information, the Student Conduct Procedure, which apply to students undertaking a Degree Apprenticeship Programme, can be found HERE.

39. Staff members who wish to bring a complaint about how this policy is implied to them should discuss the matter with their line manager in the first instance. Staff members may also contact Human Resources by sending an email to hr@corndel.com.

40. Students undertaking a Degree Apprenticeship Programme, who wish to bring a complaint about how this policy is implied to them should discuss the matter with their Professional Development Expert in the first instance. Students undertaking a Degree Apprenticeship Programme can also refer to the Student Complaint Procedure.

Appendix A: Guidance for Employees

Keeping your Device (Laptop and Mobile Phone) Safe and Secure

- **Never leave your laptop or phone unattended** when working or travelling off-site.
- **Avoid publicising your device**: Use a regular bag or backpack to carry it discreetly (ensure the laptop is in its protective case inside).
- **If you must leave devices in a car during the day**, ensure they devices are hidden, and the vehicle is securely locked.
- **Do not leave devices in a car overnight**, even in the boot.
- **Be aware of theft risks**: Stay alert, especially in public places, and never resist if confronted.

- **Keep your device out of sight in vehicles**: Store it out of sight and lock the doors, especially when stopping at traffic lights.

Preventing damages to your mobile laptop

- **Use a proper laptop case** for protection when carrying it.
- **Avoid unsuitable bags** and never pack it with drinks or liquids.
- **Keep drinks away** from the laptop at all times.
- **Do not use the laptop while walking** or in unstable positions.
- **Always close the lid** when not in use, even briefly, to prevent accidents.
- **Secure the laptop** when transporting it in a car or on public transport.
- **Remove objects from the keyboard** before closing the lid to avoid screen damage.
- **Never lift the laptop by the screen**, as it can damage the hinges.
- **Do not attempt to disassemble** the laptop—repairs should be done by professionals.

***Please Note**: Damage from careless use may not be covered by insurance and could result in charges to the staff member.