

# IT facilities, Internet and WiFi Policy

<b>Owner</b>	Chief Technology Officer		
<b>Version</b>	3.1		
<b>Changes</b>	Removal of restrictions that could interfere with freedom of speech, in line with OfS Regulatory advice 24 Guidance related to freedom of speech		
<b>Approval date</b>	August 2025	<b>Approved by</b>	Board of Directors
<b>Implementation date</b>	September 2025	<b>Date of next review</b>	July 2028
<b>Related internal policy</b>	Social Media Policy Student Safeguarding, Prevent and Harassment Policy Code of Practice on Freedom of Speech		
<b>Related external policies and regulations</b>	UK General Data Protection Regulation (UK GDPR) Data Protection Act (2018) Equality Act (2010) OfS Regulatory advice 24 Guidance related to freedom of speech Counter-Terrorism and Security Act 2015 Computer Misuse Act (1990) Copyright, Designs and Patents Acts		

## Contents

Introduction .....	2
Freedom of Speech .....	2
Access to the service using own device .....	3
Using memory sticks .....	4
Student Acceptable Use Policy .....	4
Use of College IT facilities .....	5
Use of College email .....	6
Appropriate use .....	6
Social Media .....	7
Monitoring .....	7
Legal framework.....	8

## Introduction

Information Communication and Mobile Technology is an accepted part of Regent College London (the College) life. It offers a valuable resource for use in the classroom and has numerous educational opportunities from photographing notes for use later to browsing the Internet. As with all technology it can present risks if used inappropriately. The College embraces technology, but within the safety of an agreed usage policy and some simple boundaries.

These boundaries form part of our response to the Prevent duty, introduced under the Counter-Terrorism and Security Act 2015, but also operate in alignment with the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (2018) and the Equality Act (2010).

It is essential that students and staff are aware that the College will not permit the usage of its internet connection for the sending or downloading of any obscene, racist, sexist, homophobic or extremist information, and that the College actively promotes an environment of tolerance and understanding to all groups.

Throughout this policy, the word device is used to describe any mobile phone, tablet computer, laptop, music player or other device capable of communicating with either the Internet and/or mobile telephone networks and/or taking video/photographs/sound recordings and all and any are included within this policy.

This policy covers the use of and liability for all devices within Regent College London and the College grounds and is in addition to policies governing student and staff behaviour and responsibilities.

This Policy supports the College in meeting the OfS Conditions of Registration. In particular, Condition B2:

The provider must take all reasonable steps to ensure:

each cohort of students registered on each higher education course receives resources and support which are sufficient for the purpose of ensuring:

- i. a high quality academic experience for those students; and
- ii. those students succeed in and beyond higher education; and

effective engagement with each cohort of students which is sufficient for the purpose of ensuring:

- i. a high quality academic experience for those students; and
- ii. those students succeed in and beyond higher education.

## Freedom of Speech

Regent College London believes that 'the end result of education is character'. To that end, we wish to establish and maintain an inclusive community that recognises

that people with different backgrounds, experience, skills, attitudes, beliefs and views bring fresh ideas and new perspectives.

The law protects the rights of members of the College to engage in debate and argument about social, political, religious, economic and scientific ideas, provided that the views expressed are not contrary to law. Freedom of speech within the law may include speech that is shocking, disturbing or offensive.

Regent College London's full Code of Practice on Freedom of Speech is available on its website: <https://www.rcl.ac.uk/about/policies/>

### **Access to the service using own device**

Use of personal devices is at the discretion of the College and should not be seen as a right.

Students' own devices can be used in the classroom at the lecturer's discretion.

All personal devices shall only contact the Internet and local area network via the College wireless network. All internet access via the network is logged.

Students are not permitted under any circumstances to access material which may be seen as extremist or terrorist in nature, or which may lead to any forms of radicalisation amongst the student populace.

The use of cameras and recording equipment, including those which may be built into certain devices, to make images or sound recordings of individuals, is prohibited unless with prior permission of any individual(s) being photographed/recorded.

The College does not approve any apps or updates that may be downloaded onto any device whilst using the College's wireless network and such activity is undertaken at the owner's risk, with the College having no liability for any consequent loss of data or damage to the individual's device. We encourage users to protect their own devices e.g. with the use of password and/or PIN as appropriate. Students are responsible for the use of their own device(s) while on the College site.

Privately-owned devices should not be used in a manner that would portray the College in an unfavourable light.

Devices should not be used to intimidate, abuse or perform any unfavourable acts against, staff, students or any person associated with the College. Any costs/fees incurred while using devices are not chargeable against the College and are the sole responsibility of the owner.

When on the College site and switched on, all such devices must be set to silent.

Charging devices in the College must only be performed using Charging Stations provided within Student Common Area. Devices must be set to silent when charging.

It is not permissible to charge own devices by unplugging any College devices from the sockets/extension leads.

Regent College London takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the College premises that is not the property of the College. If a device is stolen or damaged while on College premises, it is to be reported to reception immediately, in order that the incident can be logged. We will investigate the theft of the device not the loss.

### **Using memory sticks**

A memory stick must be treated as a “transportation medium” only and should never be considered as external data storage. The physical construction of a USB stick makes it a fragile and easy to corrupt device – especially during quick removal from a USB port. Information stored on a memory stick is not secure so a copy of the information should always be stored on the College network drive or OneDrive (part of the Office365 package).

### **Student Acceptable Use Policy**

Students must use the College Wi-Fi system in a responsible way, to ensure that there is no risk to their own safety or to the safety and security of other users.

Students need to understand that the College operates in alignment and in agreement with the requirements of the UK GDPR, the Data Protection Act (2018), the Equality Act (2010), and the Counter-Terrorism and Security Act (2015).

Students understand that the College will monitor any use of the systems, devices and digital communications provided within College premises.

Personal safety is in the hands of each individual when working on-line; students must keep passwords safe and secure – not share them, nor try to use any other person’s username and password. All learners need to understand that they should not write down or store a password where it is possible that someone may steal it.

The College believes that everyone has equal rights to use technology as a resource and that:

- College systems and devices are primarily intended for educational use and that they should not be used for personal or recreational use unless with permission.
- Students must not try (unless with permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- Students will not use the College systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting.
- Students must respect others’ work and property and will not access, copy, remove or
- otherwise alter any other user’s files, without the owner’s knowledge and permission.

- Students must not install or attempt to install or store programmes of any type on any College device, nor try to alter computer settings.

The following three measures affect levels of personal privacy and accountability:

- Students must be careful about the internet sites they access and the links contained therein; they may be investigated if those sites or links break any law or statute inscribed within the British constitution.
- Students are encouraged to be polite and responsible when communicating with others, not use strong, aggressive or inappropriate language and appreciate that others may have different opinions from themselves, and that they have a right to those opinions.
- Students must not take or distribute images of anyone without their permission.

Students need to recognise that the College has a responsibility to maintain the security and integrity of the technology it offers, and that the College has a duty to ensure the smooth running of such provision, without harm or detrimental effect. Students are responsible for all of their own actions, both in and out of College, and that the College has the right to take action against them if they are involved in incidents of inappropriate or unacceptable behaviour as covered in this agreement, whether they are in the College, or out of College and seen as members of the College community.

Any breach of this policy will result in students being subject to disciplinary action. This may include loss of access to the College network / internet, suspension, or withdrawal from the course

### **Use of College IT facilities**

Regent College London provides computers and computer equipment for the legitimate business purposes of students and staff. As such, their use for prohibited conduct will be treated very seriously and may result in your dismissal without notice. The examples of prohibited conduct detailed below are non-exhaustive.

The Group strictly prohibits the use of our computers, computer equipment, office equipment, email or internet systems to access, view, create, post, download, store, send, print, copy or distribute:

- Illegal material;
- Pornographic material of any kind or material of a sexual nature;
- Obscene material;
- Discriminatory, defamatory, harassing, derogatory or insulting material;
- Confidential or sensitive Group material unless authorised to do so.

The following actions are also prohibited:

- Generating or otherwise participating in the distribution of a virus;
- Copying software;
- Using Group programs and software for any unauthorised use;

- Using Group software or design programs for unauthorised use;
- Uploading, downloading, opening or distributing unauthorised software;
- Infringing the trademark and/or licensing rights of this Group or any other individual or organisation;
- Infringing the copyright of any individual or organisation.

### **Use of College email**

The College recognises that email is a useful tool for education and business purposes. However, it is crucial that it is used in a responsible manner at all times, whether being sent from a computer or mobile device. All students and staff are required to comply with the rules set out below.

- At no time should email be used for Prohibited Conduct.
- Sending and responding to junk email chain letters/emails is forbidden.
- It is your responsibility to ensure that you have sufficient space in your 'Inbox' to enable you to receive emails at all times. You should regularly electronically archive old emails to ensure that your email account is able to function efficiently. This will ensure you never miss vital information regarding your course of study, including assignment deadlines.

### **Appropriate use**

The College's computers and equipment are provided for the legitimate educational purposes of students and staff. As such, their use for prohibited conduct will be treated very seriously and may result in the Disciplinary Procedure being instigated. The examples of inappropriate use detailed below are non-exhaustive.

- Sending abusive or defamatory messages that could constitute bullying or harassment.
- Transmitting libellous, slanderous, threatening or abusive messages, or any messages that may be construed as such.
- Compiling or distributing chain letters.
- Visiting and viewing pornographic or other inappropriate websites. Downloading, transmission, and possession of pornographic and sexually explicit materials.
- Downloading or distributing COPYRIGHT information or software.
- Statements about other people and companies should be restricted to comments that they would not object to seeing – Remember that they have the right to view the information under the UK GDPR.
- Students must not participate in the obtaining or distribution of material that is illegal, obscene or sexually explicit.
- Students must not commit activities of an illegal or fraudulent nature, which may result in criminal prosecution. There may be personal liability for all costs and damages attributable to these activities or disruptions caused.
- Internet communications may not be used for the creation of legal or contractual obligations.

- The retrieval of executable files from the Internet is prohibited unless the Internet Administrator has given express permission. Such actions can lead to the introduction of viruses or pirated, unlicensed programs.
- Do not transmit proprietary or confidential materials over the Internet unless properly encrypted. If in doubt ask the "data owner" about the sensitivity of the data and use the appropriate methods of data protection if transmission is still necessary (consult IT Admin about encryption of e-mails).
- At no time are students permitted to use the College's computers, computer equipment or internet to participate in on line gambling of any kind.

Although material may be available for 'free' on the Internet, you may not have the legal right to copy it. Compare the Internet to a bookstore – you are free to browse as much as you like, but you are not welcome to make copies. You may need to obtain the COPYRIGHT holder's written permission before copying from the Internet or other public computer system, if the material is not explicitly made available for copying.

The Internet connection is a shared resource. While most activities won't impact other users, large file transfers and intensive multimedia activities will impact the service levels of other users. Users contemplating large file transfers should be considerate to other users and schedule these activities early or late in the day or after business hours.

Downloading of programmes/utilities from the Internet is not permitted without the express consent of the Technical Infrastructure Support. In addition to controlling unlicensed software, this preventative action will restrict virus infection at the College.

Always make a reasonable attempt to close down the browser when finished using the Internet. This will help prevent potential breaches of security.

Immediately inform the College's Technical Infrastructure Support or Senior Management of any communication, system problem or other circumstance that you think may indicate a breach of security or other risk to the integrity of the College's systems.

Passwords are confidential and should never be given to another person. If you believe your password has been copied, you should immediately inform the College's Technical Infrastructure Support.

## **Social Media**

The College's Policy on the use of social media by staff and students is available on the website: <https://www.rcl.ac.uk/about/policies/>

## **Monitoring**

Use of the College computers and IT systems (including internet and email) are monitored. This also includes personal use of them. Monitoring is carried out lawfully and to the extent that it is necessary for business purposes. To ensure monitoring is justified, the College has carried out an impact assessment.

The College reserves the right to carry out monitoring for the following (non-exhaustive) purposes:

- To prevent or detect crime;
- To comply with any legal obligations;
- To monitor compliance with College policies;
- To investigate alleged or suspected wrongful acts;
- To secure effective system operation.

Monitoring is carried out continually using automated software. Monitoring can consist of random spot checks. Monitoring of emails is usually confined to address or heading, unless it is necessary for good reason to access the content. The Senior Management team have authority to carry out monitoring. Information obtained by monitoring may be used as part of the Disciplinary Procedure.

## **Legal framework**

Regent College London has legal responsibilities regarding provision and use of computing and IT facilities. The following points of law are particularly pertinent to this Policy:

### Computer Misuse Act (1990)

It is likely that any material, which incites, encourages or enables others to gain unauthorised access to a computer system, would be found illegal under the Act.

### Copyright, Designs and Patents Acts

In general, these various Acts require that the permission of the owner of the intellectual property MUST be sought before any use of it is made whatsoever. It should be noted that the College logo and title are the property of Regent Group and they, together with addresses, may only be used with express permission.

### UK General Data Protection Regulation

This provides protection of data, which is stored in a computer or other electronic information system, that relates to any living person. The permission of each data subject should be sought and obtained before any information, including photographs, relating to them is stored in the system and/or shared with any third parties.

### Libel

Facts concerning individuals or organisations must be accurate and verifiable and views or opinions must not portray their subjects in any way, which could damage their reputation.

### Racial Discrimination

Any material that either discriminates or encourages discrimination on racial or ethnic grounds, contravenes the Race Relations Act.

### Sexual Discrimination

Any material which discriminates against any person on the grounds of sex, gender and, in some instances, sexual orientation, or encourages such discrimination, contravenes the Sex Discrimination Act

### Advertising

If advertisements are placed then they must comply with the Code of Practice issued by the Advertising Standards Authority, which requires that all advertisements should be "legal, decent, truthful and honest".