



## **Acceptable Use of IT Policy (Students)**

**September 2023**

**Review: September 2024**

## **1 Introduction**

- 1.1 Information and Communication Technology has a significant role within Reigate College both as an educational tool and for administration and communication between staff, students and the larger world.
- 1.2 In providing these facilities Reigate College must ensure that the system is used in a manner appropriate to the aims of the institution. It seeks to ensure that:
- IT Resources and student time are used effectively.
  - Our duty of care for our students is fulfilled.
  - Government lead legislation (including PREVENT and CPA guidelines) are observed and followed.
  - The reputation of Reigate College is not jeopardised by inappropriate uses of electronic communication.
- 1.3 This policy seeks to make clear what is, and what is not, acceptable. It is not the intention that this policy should be used to limit academic freedom but that Information Technology resources should be used in a manner that is legal, ethical, appropriate to the aims of Reigate College, and not to the detriment of your learning experience.
- 1.4 The College has a duty to safeguard students, to work within Keeping Children Safety in Education 2023 and the Prevent duty. If concerns are raised around IT usage and a student is accessing extremist or other potentially harmful materials online, the safeguarding and Prevent protocols would apply. The College would have an obligation to share our concerns with other agencies, such as Children's Services and Channel.

## **2 General Points**

- 2.1 The phrase 'IT Resources' as used in College policies, are interpreted as including any computer hardware, printers, telephones, network infrastructure learning platforms or software owned, operated or provided by Reigate College, including any allocation of memory/disk space on any of Reigate College owned/operated systems.
- 2.2 Users may only use those systems listed in 1.1 at Reigate College or remotely if they have signed this Acceptable Use Policy.
- 2.3 Reigate College has the right to monitor any/all aspects of its computer, network and telephone system that are made available to users and to monitor and/or document any communications made by users, including those by telephone, email and other internet communication. Reigate College also wishes to make users aware that security cameras, including facial recognition software, are in operation around the site for the protection of both our students and staff.

- 2.4 Computers and email accounts are the property of Reigate College and are designed to assist in the performance of your studies. You should, therefore, have no expectation of privacy in any communications sent or received, whether it is of a college or personal nature.

### **3 User Account Security**

- 3.1 To use the IT Resources of Reigate College a person must first be provided with their own username by IT Support. Registration to use the computer facilities implies, and is conditional upon, acceptance of this Acceptable Use Policy.
- 3.2 All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. Passwords protect Reigate College's systems from access by unauthorised people; they protect your work and Reigate College's information. The user is personally responsible and accountable for all activities carried out under their username.
- 3.3 The password associated with a personal username must not be divulged to another person. Attempts to access, or use, any username or other data, which is not authorised to the user are prohibited. The password **must** be changed on the first time of logging into the College IT system and must meet IT password protection protocols.

### **4 Use of Email, Internet and Social Media**

- 4.1 Reigate College's email system is provided to aid users with their studies. Personal use of the email system is permitted within reason, but the account is only valid whilst you are a student at Reigate College.
- 4.2 All use of the Internet can be tracked and users should be aware that all sites accessed are automatically recorded. It is important to note that if you connect your device to our guest wireless system then again, all traffic is monitored and logged. Therefore, devices that connect to the college Wi-Fi system will be monitored through software that protects users through digital safeguarding.
- 4.3 Extensive filtering and firewall appliances are in place to protect our users. In addition, users should not attempt to download, transmit or store any material that might reasonably be obscene, abusive, sexist, racist or defamatory. Any attempts to access unsuitable materials and/or circumnavigate the filtering and firewalls are automatically reported to senior staff and appropriate disciplinary procedures will be undertaken.

- 4.4 Copyright and licensing conditions must be observed when downloading from the internet. Breach of these conditions can result in legal proceedings against the college and is constituted as gross misconduct.
- 4.5 Social media is not anonymous, and the internet remembers everything. Postings of all types can typically be traced back to their authors, and information posted through social media is backed up, replicated, linked and reposted continuously. Please be conscious of how your interactions and behaviour reflect on yourself and the college.
- 4.6 Inappropriate or inaccurate comments which are damaging to a person's reputation should be avoided. Bullying/cyber bullying remains bullying even if it is not conducted in a public sphere. Think carefully about posting anything which you would not want a third party such as a future employer, institution or professional body to read.
- 4.7 In line with Keeping Children Safe in Education Guidance 2023 it is an offence of a person under the age of 18 to create, share or be in possession of nude and semi-nude pictures. Reigate College's Designated Safeguarding Lead (DSL) will be informed of all cases covering all students who attend the College.

## **5 Security & Anti-Virus**

- 5.1 Antivirus software is loaded on all computers as standard and is updated regularly via the network. There are restrictions in place to prevent users from attempting to remove or deactivate the Antivirus software, so please do not attempt to do so.
- 5.2 If you suspect that a virus has infected a computer or device on the college network then stop using the computer and contact IT Support immediately. As soon as a virus is detected on a device (including external media such as a USB drive), IT Support are immediately emailed and an automatic clean-up is attempted.

## **6 Implementation & Updates of the Policy**

- 6.1 The Associate Director (IT Systems) is responsible for the management of all College IT systems. The IT Support Department are available to give advice on the practical implications of this policy.
- 6.2 Training resources are available via the SharePoint learning platform to familiarise students with Reigate College IT system and its uses.
- 6.3 In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all users will be made when updates are available.

## **7 Disciplinary Procedure**

- 7.1 Any student whose actions are in breach of this Policy will be subject to the normal disciplinary procedures that apply to other student conduct policies. Extreme cases could be considered as Gross Misconduct and may therefore lead to permanent exclusion and/or the involvement of external bodies/agencies.