



## **Social Media Policy for Students**

**January 2021**

**Review: July 2022**

## **1.0 Aims and objectives**

- 1.1 This policy aims to outline the responsibilities of students when accessing social media either personally or using it for College purposes and to ensure that its use is acceptable to avoid bringing the College into disrepute. It aims to support the ~~aims~~ of the College policy on Student Acceptable Use of IT and the Student Code of Conduct.
- 1.2 Social media is the term used to describe the online tools, websites and interactive media that enable users to interact with each other in various ways, through sharing information, opinions, knowledge and interests (see Appendix 1 – Glossary of Terms).
- 1.3 The College recognises the value that social media can have to a student’s studies if used in a responsible and professional way. While it is recognised that students are entitled to a private life, the College is committed to maintaining confidentiality and professionalism at all times whilst also upholding its reputation by ensuring students and employees exhibit acceptable behaviours and are fully informed at all times about their rights and responsibilities for their own protection.

## **2.0 Scope**

- 2.1 This policy applies to all students at the College. There is a similar Policy which applies to Staff.
- 2.2 Individuals are personally accountable for their behaviour and may be held liable for any breaches of this policy. All students are therefore expected to support the College’s policy on social media.

## **3.0 Legislation**

- 3.1 The College will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which are predominantly the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Communications Act 2003; GDPR; the Protection from Harassment Order 1998 and the Equality Act 2010.

## **4.0 Data protection and monitoring**

- 4.1 Computers are the property of the College and are primarily designed to assist in the performance of education and business duties. To ensure appropriate use of the internet, the College’s internet software monitors all websites visited by students. Therefore, students should have no expectation of privacy when it comes to the sites they access from College computers and devices.
- 4.2 The College may exercise its rights to intercept internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:
  - To establish the existence of facts relevant to the College’s business.
  - To ascertain compliance with regulatory practices or procedures relevant to the College.
  - To ensure that students using the system are achieving the standards required.
  - To prevent or detect crime.
  - To investigate or detect the unauthorised use or abuse of the telecommunications systems, including using social media websites.

- To ensure effective operation of systems, e.g. to detect computer viruses and to maintain an adequate level of security.
- To be able to exercise its rights, the College must make all reasonable efforts to inform every person who may use the internet systems that monitoring may take place. The communication of this policy to all students meets this requirement and this policy will be displayed on Moodle and the Portal.

## **5.0 Privacy settings and personal information**

- 5.1 Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Information available on social media sites could be produced as evidence by either the College or employee or student, should it be necessary, either as part of College procedures, or in legal proceedings.
- 5.2 Therefore, it is vital that employees and students are strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access the information on those sites. Even if privacy and security settings are utilised, anything posted on social media sites may be made public by onward transmission.
- 5.3 Social media offers the ability to share personal information rapidly and easily. Students should be aware of the College Acceptable Use of IT Policy, particularly with regard to protecting passwords and personal information to reduce the risks of abuses such as identity theft.
- 5.4 To avoid identity theft, students are advised to refrain from publishing any personal or sensitive information on social media websites, e.g. date of birth, home address, telephone number or any information related to personal bank accounts.

## **6.0 Acceptable use of social media at College**

- 6.1 The College IT Systems are first and foremost educational/business tools, and as such personal usage of the systems is a privilege and not a right. Students are permitted to make reasonable and appropriate use of social media websites where this is part of the normal work relating to their studies.
- 6.2 Students who are responsible for contributing to the College's social media activities should be aware at all times that they are representing the College.
- 6.3 The College accepts that students may wish to use social media channels as a way of communicating personally with the other students, the public and/or friends; however its use at College should be restricted to the terms of this policy. Students are permitted to make reasonable and appropriate use of social media websites from the College's IT network at certain times. Students should limit their use of social media to break/lunch times and/or when travelling (before and after College) unless directed to access such a site educational purposes.
- 6.4 Students may wish to use their own personal devices, (including laptops, palm-tops, hand-held devices and smart phones) to access social media websites, while at College. Students should limit their use of social media on their own personal equipment to their break/lunch times and/or when travelling and/or times when they are not on in class (before and after College) unless directed to access such a site during a lesson for educational purposes.

- 6.5 Personal use of social media should not interfere with students' studies and responsibilities. Abuse of this policy will be considered a disciplinary offence as outlined in the Student Code of Conduct.
- 6.6 Students are not permitted to video lessons in any form for their own purposes or for the purposes of others, unless in exceptional circumstances where they have asked for and been given permission to do so by the teacher. Please note even where permission has been given to video, any images should not be forwarded, shared, published, amended or placed on any electronic media platform without explicit authorisation of the person/people on the images.
- 6.7 Students cannot use 'Reigate College' in the title of any social media pages created by them, under any circumstances. Breaches of this will be treated as gross misconduct.
- 6.8 Any personal image/video taken/made by a student and shared on social media, must not be derogatory to the College in any way. Breaches of this will be treated as gross misconduct.
- 6.8 As stated in the mobile phone policy, mobile phones must not be used to film/record any teacher or student who is taking part in College activities, particularly 'live streaming' on social media. If any student breaches this, it will be treated as gross misconduct as defined in the Student's Code of Conduct.

## **7.0 Expected standards of conduct on social media websites**

### **7.1 Appropriate conduct**

- 7.11 The line between public and private, professional and personal is not always clearly defined when using social media. If a student identifies themselves as a member of the College community, when communicating within or outside the College, students must:
- Conduct themselves in accordance with other policies, procedures and the College's current Student Code of Conduct.
  - Be courteous and respectful as would be expected in any other situation.
  - Think carefully about how and what activities are carried out on social media websites.
  - Be transparent and honest. It should be made clear that the views do not represent or reflect the views of the College.
  - Remove or request the removal of any inappropriate comments, images or videos of them.

### **7.2 Inappropriate conduct**

- 7.21 While using social media in any capacity, students' actions can still damage the College's reputation.

### **7.22 When communicating in any capacity, within or outside the College/workplace, students must not conduct themselves inappropriately. The following are examples of inappropriate conduct:**

- Engaging in activities that have the potential to bring the College into disrepute.
- Breach of confidentiality by disclosing privileged, sensitive and/or confidential information.
- Making comments that could be considered to be bullying, harassing or discriminatory against any individual.
- Posting remarks which may inadvertently cause offence and constitute unlawful discrimination, harassment and/or victimisation.

- Posting or uploading inappropriate comments, images, photographs and/or video clips about anyone at or associated with the College, past or present.
- Publishing defamatory and/or knowingly false material about the College, other students or employees.
- Engaging in discussions or anything which may contravene the College's Single Equality Policy/Student Code of Conduct and may have the potential to cause serious harm to the College.
- Use of offensive, derogatory or intimidating language which may damage working relationships.
- Behaviour that would not be acceptable in any other situation.
- Knowingly accessing, viewing or downloading material which could cause offence to other people or may be illegal.
- Posting any material that breaches copyright legislation.
- Using a College email account to create a personal social media account.
- Doing anything that may conflict with the interests of the College.
- Using social media websites in any way which is deemed to be unlawful.

The above examples are not exhaustive or exclusive.

7.23 Students will be held personally liable for any material published on social media websites that compromise themselves, other students or anyone associated with the College past and present or the College.

### **7.3 Acceptance of friends**

7.31 The College encourages the positive use of social media as part of the educational process. Social media is used by many people, particularly students to communicate with their peers and the public. Students must not accept and/or invite employees of the College to be 'friends', or 'follow' on personal social media accounts or other online services, unless there is a departmental or personal account which has been created specifically and solely for academic purposes.

### **8.0 Inappropriate conduct and excessive use**

8.1 Any breach of this policy, including inappropriate conduct of the kind listed in section 7 above, or of a similar nature, and any excessive personal use of social media websites will be dealt with in accordance with the Student Code of Conduct and may also result in the withdrawal of access to social media websites/withdrawal of internet access.

8.2 All staff are aware that children with SEND and/or differences/perceived differences are more susceptible to being bullied, including online.

### **9.0 Responsibilities**

9.1 All students are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to the Pastoral Director (Interventions).

9.2 If students have concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be seen to be harassment/bullying, this should be reported to their Pastoral Director/Senior Tutor or a member of the Safeguarding Team immediately.

9.3 If appropriate the College may report an offence to the Police.

9.4 The IT Department is responsible for maintaining the College's computer systems and for supporting students in the proper usage of the systems.

9.5 This policy has been developed to work in conjunction with other key College procedures and policies including:

- Safeguarding Policy
- Single Equality Policy
- Student Code of Conduct
- Mobile Phone Policy
- Anti-Bullying & Anti-Harassment Policy

## **Appendix 1 – Glossary of Terms**

### **Website**

#### **Facebook**

A social networking service where users create personal profiles, add other users as friends and exchange messages, including automatic notifications when they update their own profile. Additionally, users may join common-interest user groups, upload photographs and videos and link to external websites of interest.

#### **Flickr**

An online community in which users share photographs with each other.

#### **Instagram**

An online photo-sharing application and social network platform. It allows users to edit and upload photos and short videos. Users can add a caption to each of their posts and use hashtags and location-based geotags to index these posts. Each post by a user appears on their followers' 'feed' and can also be viewed by the public when tagged using hashtags or geotags.

#### **LinkedIn**

A business-related social networking site mainly used for professional networking. Users maintain a list of contact details of people with whom they have some level of relationship, called connections. This list of connections can then be used to build up a contact network, follow different companies and find jobs, people and business opportunities. LinkedIn also offers the opportunity to recommend key contacts and provide individual testimonials.

#### **Myspace**

An online community of users' personal profiles. These typically include photographs, information about personal interests and blogs. Users send one another messages and socialise within the MySpace community.

#### **Snapchat**

A mobile messaging service that sends a photo or video to someone that lasts only up to 10 seconds before it disappears. During that time, the recipient can take a screen shot, and the sender is notified that it was taken.

#### **Twitter**

A micro-blogging service enabling its users to send and read publicly visible messages called tweets. Tweets are text-based posts of up to 140 characters displayed on the user's profile page. Users may subscribe to other users' tweets.

#### **YouTube**

A video-sharing website on which users can upload, share, and view videos. A wide variety of user-generated video content is displayed, including film and TV clips as well as amateur content such as video blogging.

This is not an exhaustive list of websites that may be used. Nevertheless the Policy applies to all social media platforms.

### **Term Definition**

#### **Blog**

A blog is a type of website or part of a website usually maintained by an individual with regular entries of commentary and descriptions of events (blogging). The content of a microblog is simply smaller in size.

**Comment**

A comment is a response that is often provided as an answer or reaction to a blog post or message on a social network. Comments are a primary form of two-way communication but are available to view by others.

**Follow**

A term usually applied to Twitter in which users subscribe to other users' tweets.

**Forum**

Also known as a message board, a forum is an online discussion site. It originated as the modern equivalent of a traditional bulletin board, and a technological evolution of the dialup bulletin board system.

**Friends**

In the context of Facebook, friends are those who you give access to your personal profile. Access can be restricted by certain privacy settings.

**Social Media**

Websites and applications that enable users to create and share content or to participate in social networking.