Social Media Policy for Students

Version 2

This policy applies to all NCLT settings.

CONTENTS

1.0 Aims and Objectives

New Collaborative Learning Trust (NCLT) recognises the benefits and opportunities that new technologies offer. This policy outlines the responsibilities of, and sets out the principles by which, all those who use the Trust IT infrastructure and social networking sites are expected to follow, whether on the premises or remotely. The policy applies to all students. It supports the Student IT Acceptable Usage Policy and aims to ensure that organisational risks are effectively managed in order to:
- Safeguard young people
- Protect the reputation of the Trust, staff and students
- Protect the IT infrastructure
- Encourage good practice.

2.0 Definitions and Scope

Social media is the term used to describe online tools, websites and interactive media that enable users to share information, opinions, knowledge and interests. Social networking applications include but are not limited to blogs, online discussion forums, collaborative spaces and media sharing services, such as Facebook, Twitter, Tumblr, WhatsApp, Snapchat, TikTok, etc.

The Trust is committed to maintaining confidentiality and professionalism at all times, whilst also upholding its reputation by ensuring employees and students exhibit appropriate conduct.

3.0 Data Protection and Monitoring

Computers and devices which are the property of the Trust are primarily designed to assist in the performance of work duties and to ensure the appropriate use; the Trust's internet software monitors all website visits by students for business and security purposes. Therefore, students should have no expectation of privacy when it comes to the sites they access from school/college computers and devices or from their personal devices via the school/college wired or wireless network.

The Trust 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 and the Data Protection Act 2018; the Human Rights Act 1998; the Defamation Act 1996; the Equality Act 2010 and the Computer Misuse Act 1990.

Permission should be sought from the IT Support Department to download software to avoid viruses. Security features such as firewalls are maintained by the IT Support Department.

4.0 Acceptable Use of Social Media

The Trust 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. Those responsible for contributing to the Trust's social media activities should be aware at all times that they are representing the Trust. Other than that, students should limit their use of social media to break/lunch times and/or when travelling (before and after working hours) unless directed to access such a site for educational purposes. Its use at school/college should be restricted to the terms of this policy.

The Trust accepts that students may wish to use social media channels as a way of communicating personally with the public and/or friends. Students may wish to use their own personal devices, (including laptops, handheld devices and smart phones) to access social media websites, while at school/college. Students should be aware that the terms of this policy extend to this type of use. Personal use of social media should not interfere with studies and abuse of this policy will be considered in line with our formal intervention procedures.

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, published amended or placed on any electronic media platform without explicit authorisation of the person/people on the images.

The IT Support Department is responsible for the writing, overseeing, monitoring and updating of the Trust, school and college entries on the free online encyclopedia Wikipedia in association with senior staff. No staff or student must write or edit the Trust/school/college entry. Staff and students should always contact the IT Support Department if they find errors in online encyclopedias (such as Wikipedia). relating to NCLT, an NCLT college or NCLT school /

By logging into a NCLT/New College/School computer, students will be accepting the terms and conditions of the Trust's Student IT Acceptable Usage Policy, and this policy. In relation to permitted access to social media students agree that:

- I will not browse or download anything illegal and forward or share any material that could upset anyone.
- If I do come across any such material, I will report it immediately to a member of staff.
- I will not attempt to circumvent the security and filtering system.
- I will not attempt to access any unsupervised/unauthorised chatrooms or areas.
- I will only communicate with others online sensibly.
- I will not send or encourage others to send abusive messages through e-mail or other services.
- I will make sure that any online or offline activity will not cause the school/college/Trust staff, or any other user distress or embarrassment.
- I know that all use of the network is monitored if abuse is suspected.
- I will only take, store and use images of children, young people, and/or staff for an agreed project or purpose.

- I will only use images outside the network if I have permission from the people in the image and a member of staff.
- I will only use images that have been approved by a member of staff.
- I acknowledge that my teachers and support staff have read access to my documents and can access them for the purpose of marking work or investigating suspected issues.
- I have read and fully understand the terms and conditions of the policy agreement, and I agree to abide by the conditions.
- I understand abuse of this policy will be considered a disciplinary offence.

5.0 <u>Privacy Settings and Personal Information</u>

Default privacy settings for some social media websites allow some information to be shared beyond the individual's contacts. All students should be mindful of the information they disclose on social networking sites. Through the open nature of such sites, it is also possible for third parties to collate vast amounts of information.

In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. The IT Support Department would be happy to assist anyone who is unsure how to do this.

6.0 <u>Responsibilities</u>

All students are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to their Progress Tutor/Pastoral Leader/Safeguarding leader. 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, they should also report this to the above immediately. If appropriate, the Trust may report an offence to the Police.

The IT Support Department is responsible for maintaining the computer systems and for supporting staff and students in the proper usage of the systems.

It is the responsibility of students to choose a strong and secure password which meets the requirements of the Trust's *Student IT Acceptable Usage Policy*.

7.0 <u>Appropriate Conduct</u>

All students should ensure they adhere to the following points;

- Students should not use social media and the internet in any way to attack insult, abuse or defame other students, their family members, members of staff or bring the Trust/school/college into disrepute.

- Students should not post content that may be viewed as racist, homophobic, bigoted or demeaning to a particular group of individuals.
- Students should not post/transfer messages/images that are sexual in nature, depict graphic violence or which may offend on the basis of race, sex, religion, national or ethnic origin, disability, sexual orientation, gender identity or gender expression.
- Students should not have any contact with any member of staff through any personal social media.
- Be mindful that any posts that you make using social media sites are generally in the public domain for a long time and can be accessible by future universities or employers and this may hinder your future progression.
- If your social media profile states that you are a student at any NCLT college or school, it should also state that the views expressed are your own and do not represent the Trust/school/college.

8.0   Relationships on Social Media Websites

Our Trust/school/college use official social media accounts. Students must not accept and/or invite employees of the Trust to be 'friends' on personal social media accounts or other online services,. and must not interact with staff on any open social media platforms such as TikTok or Twitter.

An exception to this would be in the case where an immediate family member is an NCLT employee/volunteer, and this should be brought to the attention of your Progress Tutor/Designated Safeguarding Lead/Pastoral Leader immediately.

WhatsApp communication between staff and students is not authorised. Communication of teaching resources should only be carried out through the Trust approved services (e.g. Teams/Google Classroom .). The Trust's policy is that communication through its official Facebook, Instagram, Teams accounts etc. are for school/college teaching resources only. These accounts receive prior approval from the GDPR Team /Head of School or Department. Personal accounts should not be used for school/college purposes.

Where a student has unknowingly interacted with a member of staff on social media, the Trust would expect there to be a disclosure made to Human Resources immediately the situation becomes apparent, and the interaction discontinued straight away.