



Social Media Policy

Responsibility of:
Date of Approval:
Review Cycle:

IT Manager
1st September 2016
Every 3 years

Aims and Objectives

NCLT recognises the benefits and opportunities which new technologies offer. This policy outlines the responsibilities of and sets out the principles by which all those who use the trust and college IT infrastructure and social networking sites are expected to follow, whether on the premises or remotely. The policy applies to all employees, students, contractors and volunteers. It supports the Acceptable Use Policy and Staff and Student Codes of Conduct and aims to ensure that organisational risks are effectively managed in order to:

- Safeguard young people
- Protect the reputation of the trust and its colleges, staff and students
- Protect the IT infrastructure
- Encourage good practice.

Definitions and Scope

Social media is the term used to describe the 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 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.

This policy applies to all students at college's within the trust, including those on higher education courses.

Data Protection and Monitoring

Computers and devices which are the property of the trust/college are primarily designed to assist in the performance of work duties and to ensure the appropriate use, the trust/college's internet software monitors all website visits by employees and students for business and security purposes. Therefore, staff and students should have no expectation of privacy when it comes to the sites they access from college computers and devices or from their personal devices via the 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; Data Protection Act 1998; the Human Rights Act 1998; the Defamation Act 1996 and the Equality Act 2010.

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

Acceptable Use of Social Media

The trust/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 and staff are permitted to make reasonable and appropriate use of social media websites where this is part of the normal work relating to their work or studies. Those responsible for contributing to the trust/college's social media activities should be aware at all times that they are representing the trust. Other than that, staff and 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 for educational or work purposes. Its use at college should be restricted to the terms of this policy.

The trust accepts that students and staff may wish to use social media channels as a way of communicating personally with the public and/or friends. Staff and students may wish to use their own personal devices, (including laptops, handheld devices and smart phones) to access social media websites, while at college. Staff and 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 or work and abuse of this policy will be considered a disciplinary offence as outlined in the Student/Staff Code of Conduct.

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.

When staff use blogs to discuss their work, they must ensure that confidential information is not revealed. This might include aspects of trust/college policy or details of internal discussions. If in doubt about what might be confidential, staff members should consult their line manager. If a blog makes it clear that the author works for NCLT or a College, it should include a simple and visible disclaimer such as "these are my personal views and not those of NCLT". Staff members who already have a personal blog or website, or are considering starting blogging, and which indicates in any way that they work at the trust/College should discuss any potential conflicts of interest with their line manager who should then inform the IT Support Department.

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

Abuse of this policy will be considered a disciplinary offence.

Privacy Settings and Personal Information

Default privacy settings for some social media websites allow some information to be shared beyond the individual's contacts. All staff and 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.

Responsibilities

All staff and students are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to their Progress Tutor in the case of students and their line manager or Human Resources in the case of staff. If staff or 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 also report this to the above immediately. If appropriate the trust/college 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.

Appropriate Conduct

The line between public and private, professional and personal is not always clearly defined when using social media. If an individual identifies themselves as a member of the trust/college, this has the potential to create perceptions about the trust/college to a range of external audiences and also among other colleagues, students and friends.

When communicating either in a professional or personal capacity, within or outside the workplace, employees and students must:

- Conduct themselves in accordance with other policies, procedures and the Code of Conduct.
- Be professional, 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. The trust will not tolerate employees/students making false representations. If employees/students express personal views, it should be made clear that the views do not represent or reflect the views of the trust/college.
- Be considerate to their colleagues/students and should not post information when they have been asked not to. They should also remove information about a colleague/peer if that colleague/peer asks them to do so.

The following are examples of inappropriate conduct:

- Engaging in activities that have the potential to bring the trust/college into disrepute or that may have the potential to cause serious harm to the business.
- Breach of confidentiality by disclosing any personal information.
- Making comments that could be considered to be bullying, harassing or discriminatory.
- 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 colleagues, ex-colleagues, governors, students or ex-students, parents or clients.

- Publish defamatory and/or knowingly false material about the trust/college, other employees/students.
- Engaging in discussions or anything which may contravene the colleges Single Equality Scheme.
- Use of offensive, derogatory or intimidating language which may damage working relationship.
- Pursuing personal relationships with any current students or ex-students for 2 years after them leaving college.
- Participating in any activity which may compromise the individual's position at the trust/college.
- 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.
- Doing anything that may conflict with the interest of the trust/college.
- Using social media website in any way which is deemed to be unlawful.

The above examples are not exhaustive or exclusive. Any breach of this policy and any excessive personal use of social media websites will be dealt with in accordance with the trust disciplinary procedure. Information available on social media sites could be produced as evidence by either the trust/college or employee/student, should it be necessary either as part of the college procedures or in legal proceedings.

Relationships on Social Media Websites

Social media is used by many people, particularly students to communicate with their peers and the public and by the trust/college itself on official, rather than personal pages of websites such as Facebook. However, in the same way that staff would not pass on their personal address or contact details to students, employees must not form personal relationships with any students or ex-students for 2 years after them leaving college and must ensure that professional boundaries are maintained at all times. Entering in to such relationships through social media websites may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected.

An exception to this would be in the case of an immediate family member and this should be brought to the attention of your line manager immediately.

All electronic communication with students by staff should be made via the college email system or through an authorised corporate account as agreed with the IT Support Department in advance, which is secure, tracked and monitored for the safety of all concerned.

Equally, students must not accept and/or invite employees of the trust to be 'friends' on personal social media accounts or other online services, unless there is a departmental account which has been created specifically and solely for academic purposes.

Should a circumstance arise where a member of staff has unknowingly interacted with a student 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.

Staff are also advised to consider the appropriateness and impact of relationships on social media with work colleagues.