

DN COLLEGES GROUP

Social Media Policy

Effective from: May 2019

Version Number: 1

1. Purpose

- 1.1 We understand that the internet and mobile communications technology are used by our staff as a means of communication both at work and at home. The manner in which our internet facilities can be used by our staff and representatives generally is governed by our Acceptable use, Code of Conduct and other policies. This policy outlines the standards we require our staff to observe when using social media, the fact that we monitor usage of social media and the action we will take if this policy is breached.

Except where otherwise stated, this policy does not form part of any contract of employment and we may amend it at anytime.

2 Scope

- 2.1 This policy refers to 'employees' but applies to all staff including those who work on DN Colleges Group's premises, such as contract workers and volunteers.

3 Responsibilities

- 3.1 The responsibility for drafting, updating, monitoring and reviewing this policy belongs to the Safeguarding Group and it will be reviewed at appropriate intervals.

All employees are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to their line manager or the Head of People.

If you have concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be seen to be bullying, please report this to your line manager or the HR Department immediately.

The IT Department is responsible for maintaining the DN Colleges Group's computer systems and for supporting employees in the proper usage of the systems.

- **Safeguarding**
 - Taking a lead role in investigating any reported incidents.
 - Provide updates on best practice and highlighted Social Media platforms of concern.
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- **E-Safety Group**
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Approve account creation
 - Receive completed applications for Social Media accounts
- **Marketing and Curriculum leader**
 - Create the social media account following approval
 - Store social media account details, including saving passwords securely
 - Be involved in monitoring and contributing to the account
 - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training

- Regularly monitoring, updating and managing social media accounts
- Adding an appropriate disclaimer to personal accounts when naming DN Colleges Group.

4 Definitions and/or Relevant Legislation

4.1 Social Media

Social media in the context of education is underpinned by the following legislation:

- Malicious Communications Act 1988
- Communications Act 2003; Section 127
- Computer Act 1990
- The Counter Terrorism & Security Act (2015) and the Prevent Duty
- Sexting in schools and colleges: Responding to incidents and safeguarding young people. UKCCIS Guidance (2017)
- Keeping Children Safe in Education, statutory guidance for schools and colleges. Department for Education (2018)
- Working together to safeguard children, HM Government (2018)
- Sexual Offences Act 2003

In this policy, 'social media' means internet-based applications which allow users to collaborate or interact socially by creating and exchanging content, such as social networks, community sites, blogs, microblogging sites, wikis, web forums, social bookmarking services and user rating services. Examples include Facebook, LinkedIn, Yammer, YouTube, Instagram, Twitter, Tumblr, Flickr, SlideShare, Foursquare and Pinterest, the College's intranet sites as part of DN Colleges Group, and the review areas of e-commerce sites.

Social media platforms allow us to build connections and to share ideas and content more broadly and quickly than ever before, and we support their use. However, improper use of social media may give rise to a breach of your employment contract and/or our policies, and/or defamation (ie damaging the good reputation of another person or organisation), misuse of our confidential information or that of our students and/or suppliers and/or reputational damage.

This policy does not seek to regulate how staff use social media in a purely private capacity, provided that use has no bearing on DN Colleges Group or its activities. This policy is intended to ensure that staff understand the rules governing their use of social media in relation to their work for us, or when referencing DN Colleges Group, or which may affect us or our activities. It is designed to help you use these platforms and services responsibly, so as to minimise the risks set out above and to ensure consistent standards of use of social media. This policy therefore applies where:

- your use of social media relates to the DN Colleges Group or its activities;
- your use of social media relates to or is otherwise connected with your work, whether the intended use is personal or professional;
- you represent yourself, or are otherwise identifiable, as someone employed by, or otherwise associated with, DN Colleges Group.

4.2 Monitoring

Our Policy sets out DN Colleges Group's right to monitor, intercept and read communications, and applies equally to the use of social media platforms.

We will also monitor how the two colleges uses social media generally and what is said about us and about other colleges. The Marketing Team are responsible for this monitoring.

5 The Policy

5.1 Acceptable use of social media at work

The DN Colleges Group's IT Systems are first and foremost business tools and using these for personal reasons is a privilege not a right, and is subject to the restrictions set out in this policy.

Employees are permitted to make reasonable and appropriate use of social media websites where this is part of the normal duties of their work. If you are responsible for contributing to our social media activities you should remember that you are representing DN Colleges Group and follow these guidelines:

- Only interact on approved platforms about sector developments;
- clearly identify yourself, including your name and job title, and use the following disclaimer: 'The views expressed are my own and do not necessarily reflect the views of DN Colleges Group';
- ensure that all communications are of high quality (in terms of content and form) including being grammatically correct, accurate, objectively justifiable, reasonable and appropriate for the intended audience;
- not provide references or recommendations for anyone else on social media (whether employment or business recommendations) in any way that suggests any endorsement or recommendation by DN Colleges Group. If you wish to provide a reference or recommendation, you should seek advice from your line manager and ensure that any such reference or recommendation can be withdrawn at any time as we may require;
- if you become aware of adverse criticism of DN Colleges Group, inform your line manager and the Head of Marketing. Do not respond without their express approval;
- comply with the terms and conditions and policies of the social media platforms you use;
- maintain good information security practices. Use strong passwords and make appropriate use of security and privacy settings on social media platforms, and follow our email, internet and communications and information security policies, guidelines and standards;
- seek approval from your line manager before creating or exchanging comments on colleagues, students, suppliers or other colleges accounts;
- before you begin communication on a social media platform, evaluate your audience by gaining an insight into the type of content that is published and note any unwritten rules that are followed in discussions.

We accept that employees may wish to use social media channels as a way of communicating personally with the public and/or friends; however its use at work should be restricted to the terms of this policy. You are permitted to make reasonable and appropriate use of social media websites from the College's IT network during official rest breaks and/or when between appointments when travelling and/or times when you are not on duty (before and after work).

If you wish to use your own personal devices to access social media websites at work, you should limit use to your official rest breaks and/or when between appointments when travelling and/or times when you are not on duty (before and after work).

Personal use of social media should not interfere with your work duties and responsibilities. Excessive personal use of social media website and abuse of this policy will be considered a disciplinary offence.

5.2 Expected standards of conduct on social media websites

Appropriate Conduct

You must not use your work email address to sign up for personal social media websites.

You should have no expectation of privacy or confidentiality in anything you create or share on social media platforms. When you create or exchange content using social media you are making a public statement. As such, your content will not be private and can be forwarded to third parties without your consent. You should therefore consider the potential sensitivity of disclosing information (such as health information) to the world. Once sensitive or confidential information (or offensive or defamatory information) has been disclosed, it cannot be recovered and this may result in liability both for DN Colleges Group and also you personally.

Bear in mind that, even if you are using social media in a personal capacity, other users who are aware of your association with us might reasonably think that you speak on the Group's behalf. You should also bear in mind at all times any adverse impact your content might have on our reputation or customer or supplier relationships.

When creating or exchanging content on a social media platform, you must at all times comply with your contract of employment (or other contractual relationship) with us, our disciplinary rules and any of our policies that may be relevant. In particular you must:

- not harass or bully other members of staff OR breach our harassment and bullying policy;
- not promote political or social groups which are not aligned to DN Colleges Group
- not discriminate against other members of staff, students or third parties OR breach our equality policy;
- not breach our data protection, internet, email and communications, information security and/or whistleblowing policies;
- respect any confidentiality obligations owed by you or us, and not disclose commercially sensitive material or infringe any intellectual property or privacy rights of the College or any third party;
- not make defamatory or disparaging statements about DN Colleges Group, its staff or students or other colleges;
- not create or exchange or link to abusive, obscene, discriminatory, derogatory, defamatory or pornographic content;
- not upload, post or forward any content belonging to a third party unless you have that third party's consent;
- ensure that any quotes from third party material are accurate;
- check that a third party website permits you to link to it before including a link and ensure that the link makes clear to the user that the link will take them to the third party's site; and
- not post, upload, forward or post a link to chain mail, junk mail, cartoons, jokes or gossip.

You should regularly review the privacy settings on your personal social media accounts and appropriately restrict the people who can read your comments. However, even if privacy and security settings are restricted, you should be aware that anything you post on social media sites may be made public by onward transmission.

You should review the content of your personal social media accounts on a regular basis and delete anything that could reflect negatively on you in a professional capacity or on the College.

You should be honest and open but also be mindful of the impact your contribution to a site may have on the perception of the College.

If you make a mistake in a contribution, be prompt in admitting and correcting it.

Do not escalate 'heated' discussions. Try to be conciliatory and respectful and quote facts to lower the temperature and correct misrepresentations. Never contribute to a discussion if you are angry or upset; return to it later when you can contribute in a calm and rational manner.

Avoid discussing topics that may be inflammatory, such as politics or religion.

Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

The use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with DN Colleges Group's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via DN Colleges Group owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on DN Colleges Group's social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any list of those whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Acceptance of friends

DN Colleges Group 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 may wish to form personal relationships with employees, however to ensure professional boundaries are maintained, you must not accept and/or invite the following individuals to be 'friends' on personal social media accounts or other online services:

- Students of any age,
- ex-students under the age of 18, and
- parents

Entering into such relationships may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected by us. We reserve the right to take disciplinary action if employees are found to be in breach of this policy, with the potential of dismissal for serious breaches.

Acts of a criminal nature or any safeguarding concerns may be referred to the police, Local Safeguarding Children Board (LSCB) and/or the Independent Safeguarding Authority (ISA).

5.3 Use of social media during recruitment and selection process

DN Colleges Group may view relevant social media websites as part of the pre-employment process, i.e. those aimed specifically at the professional market and used for networking and career development (e.g. LinkedIn). Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

5.4 Inappropriate conduct and excessive use

We consider this policy to be extremely important. If an employee is found to be in breach of the policy, they will be disciplined in accordance with our disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct, which may lead to immediate termination of employment without notice or payment in lieu of notice. As an alternative, we may withdraw your access to social media platforms via our systems. If you are not an employee, breach of this policy may result in termination of our contract with you.

Employees should note, in particular, that creating or sharing content on a social media platform may amount to misconduct even if it takes place:

- on a personal account with appropriate privacy settings;
- outside normal working hours; and/or
- without using our computers, systems and networks.

Employees who feel that they have been harassed or bullied because of material posted or uploaded by a colleague onto a social media platform should inform their line manager or the Head of People, in accordance with our grievance procedure.

5.5 Process for creating new accounts

The college community is encouraged to consider if a social media account will help them in their communication and marketing, e.g. a Animal Management department Twitter account, or a “Promotional Facebook for The Hair Salon” Facebook page. Anyone wishing to create such an account must present a business case to the Safeguarding and E-Safety group which will involve full consultation with the Marketing team to cover the following points: -

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- The account security measures (passwords, etc)
- Will the account be open or private/closed

Following consideration by the E-Safety Group and the Marketing Team an application will be approved or rejected. In all cases, the E-Safety Group must be satisfied that anyone running a social media account on behalf of DN Colleges Group has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by DN Colleges Group, including volunteers or parents.

5.6 Declaration

All employees are required to sign to confirm that they have read and understood this policy and agree to comply with its requirements. A copy of the signed declaration will be kept in the individuals HR record and include:

I [employee full name] have read and understood the contents of the DN Colleges Group’s Social Media Policy and will comply with its requirements during my employment with DN

Colleges Group. I am fully aware of and accept that the DN Colleges Group reserves the right, in accordance with this Policy, to monitor internet usage and take appropriate action for non-compliance of this policy.

Employee signature:

Date:

6 Relevant Policies and Procedures

- 6.1
- Safeguarding Policy (2019)
 - Staff Disciplinary Policy
 - Acceptable Use of IT
 - Whistleblowing

7 Who to contact with Queries

- 7.1
- E-Learning Ambassador, phil.whitehead@northlindsey.ac.uk
 - Head of Marketing, emma.turner@northlindsey.ac.uk
 - Head of People, scott.wilson@northlindsey.ac.uk
 - Director of Digital Technologies, helen.ainsbury@don.ac.uk
 - Head of Academic Services, sarah.crossland@don.ac.uk
 - Associate Director, Safeguarding & Prevent, diane.lawson@don.ac.uk
 - Deputy Principal, kit.sargent@northlindsey.ac.uk

8 Communication

- 8.1 Internal communications eg newsletters, emails, guidance documents, staff/team meetings.

9 Authorisation

Policy Holder:	Deputy Principal
Committee Group:	Safeguarding Group
Authorising Group:	Safeguarding Group and Senior Leadership Team
Initial Authorisation:	Senior Leadership Team meeting on 03/05/19
Review Date:	Bi-annually

Appendix

Managing your personal use of Social Media:

- “Nothing” on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the DN Colleges Group logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would students or parents say about you if they could see your images?
- Know how to report a problem

Managing DN Colleges Group's social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the DN Colleges Group
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the College Group's reporting process
- Consider turning off tagging people in images where possible
- Social media using only 1-way communication is acceptable. E.G a twitter feed for news.

The Don'ts

- Don't make comments, post content or link to materials that will bring the DN Colleges Group into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of DN Colleges Group accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances
- Do not add students to social media.
- Do not have any private communication with students via any social media

E-SAFETY

Staff Do's & Don'ts

 Staff Should	 Staff Should Not
 Read the E-Safety policy and stay up to date with E-Safety issues. Be confident delivering all aspects of the E-Safety curriculum, and reflect good practice regarding internet usage as part of the professional standards.	 Post information and photos about themselves, or college-related matters, publicly that they wouldn't want employers, colleagues, pupils or parents to see.
 Use college online systems and tools in accordance with the college E-Safety & Acceptable Use Policy. Be aware that access to the College network includes monitoring, filtering and surveillance of activity.	 Befriend students or other members of the college community on social networking sites. Staff should not post information and photos of students or sensitive college activities on personal accounts.
 Know how to prevent E-safety incidents arising and what to do when one arises. Know the key websites used to report E-safety concerns, such as CEOP.	 Create their own private social media accounts to allow private two-way communication with students. Staff should not send inappropriate messages, images or any other media to students or parents; regardless of age.
 Use privacy settings and safety features to manage who can contact them and see the things you share online. Be mindful when sharing pictures or posts or liking content online which could bring your reputation into disrepute.	 Use college devices and services to keep, store or view personal and private information. Staff should not store personal phone numbers, social media accounts, documents or images on college devices.
 Have devices with a strong passcode to ensure personal data and images are secure. Also, remember to change them regularly. Staff should always log out of online accounts when leaving a device in order to secure the content.	 Use the college network & internet to access inappropriate material and content eg Extremism, Pornography, Drugs, Dating, Weapons and Hate Speech.

 Doncaster University Centre
  North Lindsey College
 DN COLLEGES GROUP

It is acknowledge that, for some staff, guidance and support in the use of alternative platforms will be necessary. With that in mind, the Academic Services team have put together a Google site, which lists approved DNCG systems, which can be used as an alternative to Facebook Groups. The site lists both Microsoft and GSuite applications, and provides video guidance on how to set-up and use each of the platforms listed. The site can be accessed by using the link below. Please note, that as this is a Google Site, the best browser to use to access the content is Google Chrome.

<https://sites.google.com/don.ac.uk/alternatives-to-facebook/home>