

Great Oaks College Social Media Policy

Person Responsible:	Richard Murr – Deputy Principal, Designated Safeguarding Lead
Date of Policy:	March 2025
Next review date:	March 2028

Rationale

Great Oaks College recognises and embraces the benefits and opportunities that social media can bring as a tool. For the purposes of this policy, social media is defined as a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. It can be used to share news, information and successes, keep staff and students up to date with important developments. Examples include Facebook, LinkedIn, YouTube, Instagram, Twitter, Flickr and Pinterest. There is, however, an inherent risk involved in using social media, in that, it is an instantaneous and far-reaching form of communication and inappropriate use can impact upon staff, students and the reputation of the College. The College encourages employees to engage, collaborate and innovate through social media; however, wherever and whenever the employee does this, they must be aware of the potential impact on both themselves and the College.

Aims

This policy is intended to minimize the risks from social media which can impact on the wellbeing of students and staff and the reputation of Great Oaks College, so that students and staff can enjoy the benefits of social networking whilst understanding the standards of conduct expected by the College. 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.

Objectives

Acceptable Use of Social Media at Work

The College IT systems are first and foremost a business tool and using these for personal reasons is a privilege not a right, and is subject to the restrictions set out in this policy. Staff contributing to the College's social media activities should remember that they are representing the College. The following rules should be followed:

- Staff should only comment within their own area of expertise to provide individual perspectives on non-confidential activities at the College.
- Employees should never represent themselves or Great Oaks College in a false or misleading way. All statements must be true and not misleading; all claims must be substantiated.
- Use common sense and common courtesy: staff should ask permission to publish or report conversations that are meant to be private or internal to the College.
- Where employees access social media for work-related purposes or personal use using the College's IT facilities and equipment, the College's e-safety Policy will apply.
- If an employee's use of social media is considered to be derogatory, discriminatory, bullying, threatening, defamatory, offensive, intimidating, harassing, creating legal liability for the College, bringing the College into disrepute, breaching College policies or causes Safeguarding concerns, then the College may take action under the staff disciplinary procedure. This may include comments, videos, or photographs, which have been posted on social media sites about the College, students, work colleagues or managers.
- The College's response to any misuse of social media in a personal capacity will be reasonable and proportionate to the perceived offence; the nature of the postings/comments made and the impact or potential impact on the College, its staff, stakeholders and/or students.
- Social networking sites may be referred to when investigating possible misconduct/gross misconduct.
- Staff should be aware of security threats and be on guard for social engineering and phishing attempts. Social networks can also be used to distribute spam and malware.

- The College accepts that employees may wish to use social media as a way of communicating personally, however its use at work should be restricted to the terms of this policy. Employees are permitted to make reasonable and appropriate use of social media websites from the College IT system during official breaks.
- The use of personal devices to access social media websites at work should be limited to official breaks and not when expected to be carrying out their work duties.

Responsibilities

- Employees should be transparent and state that they work for Great Oaks College if they are posting about the College. If you are writing about the College or a competitor, use your real name, identify that you work for the College, and be clear about your role. The College discourages staff from posting online anonymously or using pseudonyms. You should never impersonate another individual.
- Employees should 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 the College; in such cases as disclaimer stating "The views expressed are my own and do not necessarily reflect the views of the College".
- 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.
- Line managers are responsible for addressing any concerns and/or questions arising out of the use of social media and should refer to HR where the concerns may lead to disciplinary action.
- Employees are responsible for their words and actions in an online environment and are therefore advised to consider whether any comment, photograph or video they are about to post on a social networking site, is something that they would want students, colleagues and other employees of the College, their manager or people outside the College to read.
- HR and the Senior Leadership Team are responsible for giving specialist advice on the use of social media for College business. If employees become aware of any adverse criticism of the College, they should follow our whistleblowing procedures.

Appropriate Conduct

Staff may not use their work email address to sign up for personal social media websites. Staff should have no expectation of privacy or confidentiality in anything created or shared on social media platforms. When creating or exchanging content using social you are making a public statement and as such will not be private and can be forwarded to third parties without your consent. Employees are therefore encouraged to consider the sensitivity of disclosing 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 the College and you personally. Employees should also be aware that even when using social media in a personal capacity, other users may be aware of their association with the College and may reasonably think they are speaking on the College's behalf. Employees should also consider any adverse impact content posted on social media may have on the College's reputation or agency relationships.

Staff must:

- Not discriminate against any members of staff, students or third party
- Respect confidentiality obligations owed by members of staff or the College 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 the College, 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.
- Do not escalate "heated" discussions, and do not discuss topics that may be inflammatory, such as politics or religion.
- Regularly review privacy settings on personal social media accounts and review the content of your personal social media accounts and delete anything that could reflect negatively in a professional capacity or on the College.

Acceptance of Friends

Employees must not accept and/or invite the following individuals to be "friends" on personal social media accounts, closed groups or other online services:

- Students of any age
- Ex-students who have left within 3 years
- Parents/guardians/carers of students

Entering into such relationships may lead to abuse or accusations of abuse of an employee's position of trust and breach of standards of professional behaviour and conduct expected by the College. The College reserves the right to take disciplinary actions 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 must be referred to designated safeguarding leads and/or the Principal, who may report the matter to the police and or the Local Authority (LA) if appropriate. If an employee is "friends" on personal social media accounts or other online services with students of any age, ex-students under the age of 18 and/or parents due to a justified reason (for example, the person is a family member), this must be declared to your line manager.

Use of Social Media during Recruitment & Selection Process

The College may view relevant social media websites as part of the pre-employment process. Where this is done the College will act in accordance with the data protection and equality & diversity obligations.

Inappropriate Conduct and Excessive Use

If an employee is found to be in breach of this policy, they will be disciplined in accordance with our Disciplinary Policy. In certain circumstances breach of this policy may be considered gross misconduct which may lead to immediate dismissal without notice. Alternatively, the College may choose to withdraw access to social media platforms for that individual. Employees should note that creating Employees should be aware 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 or networks. The College will use the Disciplinary Policy to address issues of excessive use of social media platforms during working hours.

Social Media Account Management

All corporate social media accounts must adhere to the College's brand guidelines and the account profile information should clearly state the purpose of the account and the hours during which it is monitored. It is important that all social media accounts are kept up to date, posted from regularly and monitored on a frequent basis. Questions should be responded to promptly within operating hours. Where several members of staff require access to the same social media account, there must be an agreed overall account manager, all content must be approved by the principal. All social media accounts and account managers must be logged with the business manager

It is important that posts celebrate the diverse nature of our students. All staff have the opportunity to submit a post. Any posts will be submitted to SLT to then be checked and uploaded. All photos of students must have an accompanying permissions from parents or carers. Staff are emailed annually explaining that we may use photos of them on our social media however they have an opt out should they wish not to be featured. This should be emailed to Iwona who will share with SLT.

Other relevant policies and documents

This policy should not be read in isolation but should be cross-referenced to other relevant College employment and student policies and procedures, including:

- E-Safety Policy
- Safeguarding Policy
- IT Acceptable Use Policy
- Staff Disciplinary Policy
- Data Protection Policy and Procedure
- Keeping Children Safe in Education Part 1
- Whistleblowing policy

Annex 1

Great Oaks College Online safety agreement

Parents/carers: please read and discuss this agreement with your young person and then sign it, ask your young person to sign it, and return it to the college. If you have any questions or concerns, please speak to

Richard Murr – Deputy Principal.

Young person's agreement

- ☐ I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
- ☐ I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to the teacher.
- ☐ I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- ☐ I will not give out any personal information online, such as my name, phone number or address.
- ☐ I will not reveal my passwords to anyone.
- ☐ I will not arrange a face-to-face meeting with someone I meet online unless I have discussed this with my parents/Carers and am accompanied by a trusted person.
- ☐ If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I can talk to Rich Murr

I understand that my internet use at Great Oaks College will be monitored and logged. I understand that these rules are designed to keep me safe and that if I choose not to follow them, Great Oaks College may contact my parents/carers/Social Worker.

Signatures:


We have discussed this online safety agreement and _____ agrees to follow the rules set out above.

Parent/carer signature.....

Date

Young person's signature.....

Date

Agreed by Board of Trustees	
Print Name	Killian O'Sullivan
Sign	
Date Agreed	4th March 2025