KINGFISHER
EDUCATION GROUP

SOCIAL MEDIA POLICY

Responsible:	Director
Date Reviewed:	January 2025
Review Period:	Annually
Approval Authority:	Governors
External Release:	Yes

The rise of social media, especially social networking platforms, has opened up new avenues for media communications that significantly affect colleges. In this context, 'social media' refers to dynamic, socially interactive, and networked information and communication technologies, such as Web 2.0 sites, SMS text messaging, and social networking platforms.

Kingfisher Education has established clear guidelines and policies for various operational areas, such as human resources, IT, and corporate identity; however, these do not specifically address the use of social media.

The purpose of these social media guidelines is as follows:

- to encourage **good practice**
- **to protect** the school, it's staff and students
- to clarify where and how **existing policies** and guidelines apply to social media
- to **promote effective and innovative use** of social media as part of the school's activities.

Any official Kingfisher Education social media site or group requires approval from the Director. A comprehensive record will be maintained of all authorized sites, whether developed by students, alumni, staff members, or the marketing department for official promotional purposes. Each approved site must have a designated administrator responsible for its content.

General guidelines

All existing Kingfisher Education policies related to staff and students are applicable to social media usage. This encompasses HR policies, codes of conduct, acceptable IT use and disciplinary procedures. The following policy holds particular significance:

Kingfisher Education Safeguarding Policy and Procedures

- Any department reaching out to alumni should first consult with the Marketing office.
- It is essential for both staff and students to implement effective precautions while using social media platforms to safeguard their personal safety and guard against identity theft.
- It is important for both staff and students to take into account intellectual property rights, copyright, and data ownership when engaging with social media.
- Kingfisher Education supports staff using social media when it enhances current services; however, social media should not be employed when existing services provide similar functionality.
- When staff members use social media for personal reasons during work hours, they should adhere to the school's existing IT policies and any relevant local management directives.
- People need to be careful when engaging with and replying to potentially controversial posts on social media platforms.
- Kingfisher Education will consistently evaluate its use of social media and may adjust its policies if the status of specific social media platforms changes. This includes scenarios such

as the introduction of fees, alterations in content usage, changes in terms of use, or if a platform ceases operation.

Encouraged practice

- **Academic uses** – Kingfisher Education acknowledges that social media can enhance and promote learning opportunities, and it encourages its utilization for this purpose. However, social media should not be employed when existing learning resources or methodologies provide similar functionalities.
- **Collaborative uses** – Kingfisher Education supports both internal collaboration and external collaboration, acknowledging that social media can create opportunities for individuals and organisations to work together effectively.
- **Communications and External Relations uses** – Kingfisher Education acknowledges the potential to engage with both prospective and current customers via social media, integrating it into a comprehensive marketing strategy.
- **Prospective and current students' uses -** These users, along with others interested in the school, engage actively on social media platforms, such as creating Facebook groups and blogging. The Marketing department will keep an eye on these sites to gain deeper insights into customer needs. Any potential responses to contentious issues raised on unofficial social media sites should be directed to the Director.
- **Alumni uses** – Kingfisher Education sees the potential to engage with current students and alumni via social media to foster lasting relationships. The Marketing department is tasked with this responsibility, as they manage alumni contact information and will work closely with the Director.
- **Sports and Social Activities department** – Kingfisher Education recognises that the Sports and Social Activities department may wish to leverage social media to enhance the visibility of its services for both current and potential students. The responsibility for these initiatives lies with the Sports and Social Activities department.

Other potential uses

- Kingfisher Education will only consider social media sites for student and job applications if they are explicitly mentioned in the application. The school will evaluate all applications solely based on the information presented.
- Kingfisher Education may consider social media platforms when examining disciplinary violations such as cheating, harassment, or anti-social behavior. For more details about student disciplinary procedures, please visit the Kingfisher Education website.
- The school might keep an eye on forums and blogs to gather indirect feedback regarding its services and facilities. While the school may respond to questions or provide factual

corrections in these spaces, it generally exercises caution before engaging in controversial topics.

- Kingfisher Education retains the authority to implement any required measures to safeguard its facilities, staff, and students from malware (malicious software), which may include blocking access to sites associated with these threats.

IPR, copyright and ownership of data

Protecting IPR in your work

When sharing content on a social media platform, it’s essential to safeguard the rights associated with your work and those of Kingfisher Education. Always review the site’s terms and conditions to ensure it does not assert copyright over your posted content or claim that any content you share becomes public domain.

Typically, a website's terms and conditions will indicate that by uploading content, you grant permission for the site to publish it. This permission should be non-exclusive, meaning you can use the content elsewhere. All rights and ownership should remain with you, allowing the site only to publish your content on their platform. Additionally, you should have the ability to remove your content, which should terminate the site's rights, unless you have shared it in a way that allows it to remain on other users' profiles. Furthermore, you should have control over who can access your posted content through privacy settings or other methods, unless the site is entirely public and you are comfortable with that.

You should also take into account how sharing content on a social media platform might impact other potential uses. For example, if you post a draft of a research paper or a book, it could jeopardise your opportunities to secure a print publisher, as they may view the online post as prior publication.

IPR in the work of others

There are numerous misunderstandings regarding the application of copyright law on the internet. The matters related to copyright and other intellectual property rights are often quite complex. Generally speaking, when it comes to copyright, the best practice is to use content (such as text, images, audio, video, etc.) only if you have received explicit permission. For instance, you should avoid using an image sourced from Google Images on a Facebook page.

You may quote brief excerpts from another source for the purpose of review or commentary. However, if you intend to use content from another source, it is essential to verify that you have permission to do so. If the material is from a different website, that site may provide guidelines regarding reuse. If not, you might need to reach out to the rights holder directly.

The casual atmosphere of social media may promote a relaxed approach to rights issues; however, it's essential to keep in mind that copyright and intellectual property laws remain in effect.

Social Media uses on behalf of the Kingfisher Education - Dos and Don’ts

If you are responsible for managing social media communications for Kingfisher Education (as part of the broader marketing and PR efforts within the marketing department), please refer to the following guidelines:

DO:

1- Engage in conversation
Engaging with your audience across different social media platforms can be one of the most enjoyable aspects of establishing a brand online! Consistently participating in meaningful conversations is essential for fostering a robust dialogue with your stakeholders.

2- Ensure a brand is consistent across networks and platforms
If you create confusion among their audience, they risk losing them. It's essential to maintain a consistent 'vibe' across various social media profiles. By keeping the style and tone of voice uniform, audiences are more likely to recognize and connect with a brand.

3- Disclose relationships when endorsing an organisation/ client / customer
For instance, when a practitioner tweets (or retweets) news about a client, it's advisable to mention [client] at the end of the tweet. If a practitioner frequently shares news about their employer, it's important for them to disclose this relationship by including their employer's name in the biography section of their Twitter profile.

4- Be honest about who ‘manages’ social media channels
When updating social media accounts for individuals or organisations, it's important to be transparent. For individuals, clearly indicate who manages the account (e.g., "@person" manages this channel) in the biography or administration sections. For organisations, while it's ideal to declare the channel managers, it's not mandatory, as they typically have a vested interest in the organisation.

5- Outline content approval process from the offset
Collaborate with all parties engaged in social media activities to establish an approval process at the start of the campaign. For instance, every blog post that has been ghostwritten must receive approval from executives. Additionally, ‘a’ is authorised to regularly update the Twitter account, Facebook page, and YouTube channel without needing approval for individual tweets, status updates, or comments.

6- Be transparent when updating information
When a practitioner collaborates with a community to refresh company or client-related information, transparency about their identity and intentions is crucial. For instance, if a practitioner aims to update a Wikipedia entry on behalf of a company or client, it's advisable to visit the discussion or talk pages and collaborate with an editor to make the necessary updates. All changes and entries on Wikipedia should maintain a neutral tone, be fact-based, and verifiable. Be sure to thoroughly review the Wikipedia guidelines before submitting or editing any article.

7- Correct errors openly and in a timely manner
Always admit to errors and openly correct them. It is advisable to tackle an online crisis as soon as possible to stop it escalating out of control.

8- Add a ‘views are my own’ disclaimer where appropriate
A disclaimer is important for practitioners using personal social media accounts to share both personal and professional opinions. For instance, adding "views are my own" to a Twitter bio clarifies that personal opinions do not reflect the company's views, preventing confusion when discussing client-related news alongside personal topics.

9- Be upfront about conflicts of interest and paid for opportunities
When writing or contributing to a blog that endorses a service provider, it's essential to highlight any potential conflicts of interest. This includes disclosing any financial ties or partnership connections between the client/member and the supplier.

10- Be respectful
Always obtain permission before updating information or uploading images and videos that include colleagues or clients to any social media platforms, such as Twitter, Facebook, and YouTube, among others.

DON’T:

1- Forget that a social media presence becomes part of a brand legacy
Social media content—whether posts, pictures, images, tweets, or status updates—has the potential to remain online indefinitely. It's important to consider the message you wish to convey through your social media platforms.

2- Make an audience feel uncomfortable
Being authentic and showcasing your personality is important; however, consistently displaying a unfriendly demeanour or openly criticising others can alienate your audience and discourage them from engaging with you or your organisation.

3- Bring a company into disrepute
It's common for legally binding contracts to contain a clause that prevents employees from bringing the organisation into disrepute. It's essential to recognise that this clause applies to both online and offline behaviour. To grasp the online boundaries specific to your organisation, refer to the social media guidelines provided.

4- Reveal company / client sensitive information or intellectual property
Confidential offline information, such as new business wins, should not be shared online unless explicit permission has been obtained from the relevant parties, it serves the public interest, or it is mandated by law.

Personal Use of Social Media Sites – Policy and Procedure Purpose

The Personal Use of Social Media Sites Policy aims to guide employees on appropriate conduct when using social media. It helps minimise risks to themselves and students by preventing potential safeguarding issues, protecting employees' integrity, and maintaining the reputation of the school.

Additionally, following the policy reduces the chances of violating the Data Protection Act or facing legal issues such as libel, defamation, and copyright infringement.

Scope

The policy is appropriate to all Kingfisher Education staff.

This policy is concerned with the personal use of social media sites, not with work / official social media sites. Employees wanting to create a work-related social media site must discuss this with and obtain approval from the Director.

Principles

- Kingfisher Education ensures equality of opportunity, treating employees fairly without discrimination based on race, nationality, gender, marital status, disability, age, sexual orientation, trade union activity, political or religious beliefs, or unrelated criminal convictions.
- This policy is not intended to prevent employees from using social media sites, but to make them aware of the risks they could face when sharing information about their professional and / or personal life.
- Employees should be encouraged to report any concerns that they have regarding content placed by employees on social media sites. Employees should report their concerns to their Line Manager / the Director.

Roles and Responsibilities

Line Managers

Line Managers must ensure that all employees are familiar with the Personal Use of Social Media Sites Policy and Procedure, as well as their responsibilities related to it. It is the Line Manager's duty to investigate and address any violations of this policy, which may involve referring the matter to the Local Authority’s Safeguarding Unit.

Employees

Employees are required to follow the established policies and procedures, ensuring their conduct does not endanger children or vulnerable adults, tarnish the school's reputation, or harm their own professional standing.

Procedure

Social media sites covered

This procedure covers the use of all types of social media sites, which include but are not limited to:

- Social networking sites e.g. Facebook, MySpace and Bebo
- Blogging
- Twitter
- Video Clips and Podcasts e.g. YouTube
- Forums.

Responsibilities of employees

- Employees are accountable for their social media content, which remains public for an extended period.
- To prevent conflicts of interest, employees should not accept students under 18 or vulnerable adults as "friends."
- Information must not be posted that would disclose the identity of students.
- Students must not be discussed on social media sites.
- Images or videos featuring students or their residences should not be shared on social media platforms.
- Employees must refrain from sharing information on platforms, such as photographs and videos, that may tarnish the reputation of the school or its affiliated organisations.
- Employees are prohibited from presenting their personal views or opinions as if they represent the school or any affiliated organisations.
- Avoid posting potentially defamatory comments about Kingfisher Education, it's affiliated organisations, employees, students, their relatives, suppliers, and partner organisations on social media platforms.
- Employees are prohibited from endorsing or criticising service providers used by the school or its affiliated organisations, as well as from forming online relationships that could lead to a conflict of interest.
- Employees are required to adhere to the standards set by the Equality Act and the Human Rights Act, ensuring that they do not use any offensive or discriminatory language on social media platforms.
- Employees must not divulge any information that is confidential to the College, associated companies or a partner organisation.

Security

Employees need to exercise caution when sharing information on social media, as it can be seen by a wide audience and may reveal their workplace and associates. This exposure heightens the risk of false accusations and threats. Additionally, social media platforms could inadvertently identify children or vulnerable adults, potentially compromising their safety and security.

There is a risk of causing offense or unintentional embarrassment, such as students finding compromising photos of their teacher, potentially harming their professional reputation and that of the College. Additionally, social media can reveal employees' locations, posing security risks.

Consequently, the primary focus should be on the information shared on social media platforms. Employees are encouraged to make use of the security settings on these sites appropriately to help mitigate the aforementioned concerns.

Employee groups / networks

Employee groups can be created on social media platforms like Facebook. The creators of these groups hold the responsibility of overseeing the content shared on the site and ensuring it remains appropriate.

Disciplinary action

Employees should be aware that the use of social media sites in a manner contrary to this policy may result in disciplinary action.

Employees using social media sites must not access social media sites for personal reasons during working time.

Any instances of “cyber bullying” will be addressed in our Guidance to Dealing with Alleged Bullying Policy.

Appendix Employee guidelines 1. Introduction

With over 250 million users, Facebook is the most popular social networking site. However, it poses significant risks, as profiles often include personal information like names, addresses, and birthdates. This can facilitate identity theft and allow criminals to open credit cards in someone else's name. Such incidents are reported frequently, leading to financial loss and damage to credit ratings, which can be difficult to resolve.

Many employees use social media platforms like Facebook, Twitter, Bebo, and MySpace. This guidance aims to help employees set appropriate privacy settings on their Facebook profiles. The same principles apply to other social networking sites, so it's important to understand and adjust the default privacy settings.

2. Scope

This guidance document pertains to all social networking platforms, including but not limited to Facebook, Bebo, Twitter, and MySpace. Its purpose is not to promote the use of Facebook or similar sites, but to ensure that employees who engage with these platforms do so safely.

3. Risks

There are many risks with using Facebook. Here are some risks that you need to be aware of:

- Anyone could find out information about you through the use of Facebook.
- Threatening messages could easily be sent through the use of Facebook.
- There are risks to professionalism and independence when working with children and vulnerable service users.
- Sharing details in your status field might inadvertently reveal that you are on vacation and your home will be unoccupied for a few weeks.
- There are potential risks to children who update their status to show their whereabouts.
- Damage can be done to the school’s or associated organisations’ reputation by posting inappropriate comments on another user’s profile.
- Inappropriate photographs or offensive jokes/comments can be posted on an employee’s profile.

4. Facebook Privacy Overview

Facebook security is divided into separate parts:

- **Account Settings** – To controls username / password details and to control what information you share with others.

- **Privacy Settings -** Security settings within the website to control what information is visible on your profile e.g. basic information, personal information, photos, wall posts and searching.
- **Application Settings -** Security in relation to the functionality of applications e.g. events, groups, videos and gifts.

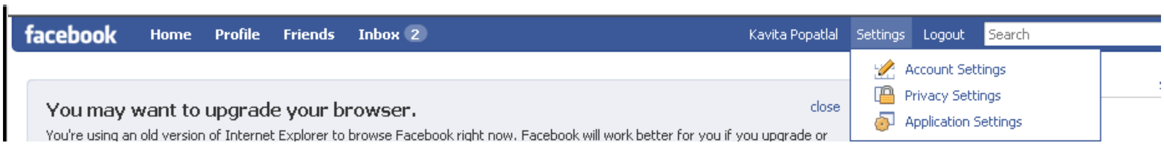
5. Account Setting Recommendations

5.1 Information entered into your profile and accepting friends' requests

To enhance your online security:

- Change your profile privacy settings to show only your birth day, not the year.
- Avoid sharing your mother's maiden name, pet's name, or school history, as these are common security questions for account verification.
- Be cautious about the information and photos you post, considering that current or future employers may view your profile.

Use Facebook's message board (your "wall") carefully, as messages exchanged are visible unless privacy settings are secured.



You may want to upgrade your browser.

You're using an old version of Internet Explorer to browse Facebook right now. Facebook will work better for you if you upgrade or

5.2

Sharing with your friends that you're going on vacation with your entire family can alert burglars to your empty home and even your return date.

Hosting a house party and inviting friends might attract uninvited guests. A notable incident occurred on a MySpace profile, where a group of strangers showed up and caused thousands of pounds in damage to a homeowner's property.

Accepting friend requests

Facebook promotes the idea of connecting with as many people as we can. As a result, some individuals might feel inclined to accept every friend request that comes their way. As a Facebook user, it's important to keep the following points in mind before accepting a friend request;

6.

Think carefully about who you allow as a friend Remember people may not be who they say they are If in doubt of a person’s identity, do not accept the request.

Security / privacy settings within the website

Facebook provides various privacy settings for controlling information sharing, but users must adjust these settings appropriately. It's crucial to explore options under privacy and avoid default settings, which may expose accounts to others. This section outlines key privacy settings on Facebook to help users manage their information sharing effectively. Take time to review and decide on the desired privacy levels.

6.1 Profile

By default, Facebook permits all your friends and networks (such as groups) to access your profile information. Since networks can include thousands of individuals, keeping this setting as is means your information will be visible to many users. Fortunately, Facebook offers privacy settings that allow you to secure your profile, with three options available for you to choose from.

- **Making your profile available to everyone**
  This will make your profile available to everyone and anyone. This is not recommended.
- **Making your profile available to your friends and networks**
  This setting allows all your friends and networks to view your profile. Friends are usually the contacts that you have created/received a request from and will only appear on your contacts list when both users have clicked “accept”.
- Your profile would be open to anyone else within your network, i.e. all the groups / networks that you have joined. Again this opens your profile to anyone else that is listed as a member.
- **Making your profile available to your friends only**
  This is the most secure option and is recommended. Other people can still search for you, but they would not be able to view your profile / photographs or comments until they are listed as a friend in your contacts list.

6.2 Search

You can adjust a setting in the privacy tab to prevent others from finding your profile in searches. Facebook's search feature allows anyone to enter your name to find users with matching names, which can then be narrowed down by various filters like location, age, and gender.

The following settings can be changed in relation to searching:

Allow anyone to see my public search listing

If you want people you know to know that you are on Facebook, leave this unselected.

Allow my public search listing to be indexed by external search engine

7.

Replying to a message or receiving a friend request temporarily allows that user to view your profile even if your normal privacy settings would not allow them to do so. This area allows you to control what profile information you wished to be visible. You should also be careful about whom you reply to. If in any doubt, you could block a user.

6.4 Block People

An option is available to block another user. They will not be able to search for you, view your profile or contact you on Facebook. Any current connections you have with that user will be removed (e.g. friendship, relationship). You can use this if you are having problems with a particular person trying to contact you.