

# Social Media Policy

| Document History    |  |                             |                                       |
|---------------------|--|-----------------------------|---------------------------------------|
| Author              | Andy Barton  | Ref and Document<br>Version | Social Media<br>Policy<br>V7_AB230925 |
| Reviewed by         | Andy Barton  | Reviewed Date               | 23/09/2025                            |
| Approval            | Board of Trustees  | Approval Date               | 06/10/2025                            |
| Next Review<br>Date | 29/09/2028   | Policy Number               | PRJ-12                                |
| Publication         | Reception; College website R:/Policies/SocialMediaPolicy.pdf |                             |                                       |

**PRJ-12** 

### Introduction

Social media is a web-based technology to facilitate social interaction between a large group of people through networked devices or computers. The most widely used network is the internet, but social media platforms are also for local networks as well. Because of the latest technological revolution, social media is still growing rapidly and becoming a vital part of everyday life. This stunning growth is due to the increasing usage of smart phones and tablets. Easy to use apps make it simple to use such devices to access any social media platform from almost anywhere.

Greenbank recognises that access to technology in the organisation gives students, parents/guardians, tutors, other staff, trustees, and clients, greater opportunities to engage, communicate, and develop skills. These skills will prepare students for work and life in general and allow a wider communication perspective in the online community. Greenbank is committed to helping students develop 21st-century technology and communication skills.

To this end, this Social Media Policy outlines the guidelines and behaviour that users are expected to follow when using social media on Greenbank's systems, or when using personally owned devices within the organisation and through its network. Particularly:

- Students, parents/guardians, teachers, clients, and staff are expected to follow the same rules for good behaviour and respectful conduct online as offline.
- Misuse of social media can result in disciplinary action.
- Greenbank makes a reasonable effort to ensure staff and students' safety and security
  online but will not be held accountable for any harm or damage that results from
  misuse of social media technologies.

We encourage students, staff, and clients to use social media (X, Facebook, etc.) as a way to connect with others, share resources, and enhance the education and work experience. While social networking is fun and valuable, there are some risks that should be kept in mind when using these tools. In the social media world, the lines are blurred between what is public or private, personal or professional.

These social media guidelines are for you to follow when representing the organisation in the virtual world.

# **Use Good Judgement**

- Greenbank expects you to use good judgment in all situations.
- You must know and follow Greenbank's Student Behaviour Policy, Greenbank's Electronic Mail, Internet and Intranet Policy, and Greenbank's Data Protection Policy.

 Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.

## Be Respectful

- Always treat others in a respectful, positive, and considerate manner.
- Do not be tempted to respond disrespectfully or inappropriately to a potentially inflammatory or offensive post by another.

## **Be Responsible**

- If you are approved to represent Greenbank, unless you are specifically authorised to speak on behalf of Greenbank as a spokesperson, you should state that the views expressed in your postings are your own. Only discuss organisation-related matters that are within your area of responsibility.
- Staff should be open about their affiliation with Greenbank and the role/position held.
- Staff are advised to not invite parents/guardians to become their 'friends' on social media. There may be a conflict of interest, and also security and privacy issues.
   Where relationships are already established, staff should proceed with caution, being fully aware of the social media guidelines and the code of conduct.
- Staff should not accept 'friend' requests from any current Greenbank student under 18 years old under any circumstances.
- Staff are advised not to invite other students to be 'friends' on social media due to a conflict of interest, as above. Where the member of staff has a connection with a student beyond the context of the organisation, it may be permissible to continue cautiously.
- Students should take care and time with posts and responses and not have a 'knee-jerk' reaction to something seen online. Care should be taken to ensure that posts are respectful to the organisation and its staff.
- Ensure that the social media accounts that are used have a strong and complex password, and that this password is kept secure.
- Take care not to allow interaction on social media to damage working relations between those who work at Greenbank, and students, parents/guardians, and clients.

## Be a Good Listener

- Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly and to share feedback.
- Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback, etc.
- Always be doing at least as much listening and responding as you do 'talking'.

# Do Not Share the Following:

Confidential Information

- Do not publish, post, or release information that is considered confidential or not for public digestion. If it seems confidential, it probably is.
- Online 'conversations' are never private. Do not use your birth date, address, and phone number on any public website.

#### Private and Personal Information

- To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules or situations.
- Never give out or transmit the personal information of students, parents, or colleagues.
- Do not take information you may receive through social networking (such as email addresses, customer names, or telephone numbers) and assume that it is the most up-to-date, or even correct at all.
- Always respect the privacy of colleagues and students.
- Identity theft is a real problem. Restrict the amount of personal information given out. Social media sites allow people to post detailed personal information such as date of birth, place of birth, and, for example, favourite football team, all of which can form the basis of security questions and passwords.

# Please be cautious with respect to:

#### Images.

- Respect brand, trademark, copyright information and/or images of the organisation.
- You may use photos and videos that are available on Greenbank's website.
- It is generally not acceptable to post pictures of students aged under 18 years without the expressed written consent of a parent or guardian.
- Do not post pictures of others (students, colleagues, etc.) without their permission.

#### Other Sites.

- A significant part of the interaction on blogs, X, Facebook, and other social networks involves passing on interesting content or linking to helpful resources.
   However, Greenbank could be ultimately responsible for any content that is shared. Do not hastily re-post a link without looking in detail at the content first.
- On a computer, pay attention to the security warnings that pop up before clicking on unfamiliar links. They actually serve a purpose - they protect you and the organisation.
- When using X, Facebook, and other tools, be sure to follow their printed terms and conditions.
- Staff, students, parents/guardians, and trustees, should not link any personal websites, social networking sites, or social media, to Greenbank's websites.

#### If you make a mistake.

- Be sure to correct any mistake you make immediately, and make it clear what you have done to fix it.
- Apologise for the mistake if the situation warrants it.
- If it is a serious mistake (such as exposing private information or reporting confidential information), staff should let a SMT (Senior Management Team) member know, and students should let their tutor or other suitable member of staff know immediately so that Greenbank can take the proper steps to help minimise the impact it may have. The matter may have to be referred to the Information Commissioner's Office (ICO).

## **Netiquette**

Users should always use the internet, network resources, and online sites in a courteous and respectful manner. Users should be aware that amongst the valuable content that there is online, there is also unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the internet.

- Users should also remember **not to post anything online that they would not want parents, tutors, colleagues, or future colleges or employers to see**. Once something is online, *it's out there* and can sometimes be shared and spread in ways that were never intended, without any real possibility of it ever being erased.
- Do not include any information that breaches copyright.
- Do not defame (libel) anyone. Anyone who makes a defamatory statement that is published on social media, or the internet in general, may be legally liable for any damage to the reputation of the individual concerned.
- Do not include any comments or material that is abusive, defamatory, sexist, racist, or that could be interpreted as harassment or bullying.
- Nothing should be posted that is illegal.

## **Personal Safety**

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety:

- **Students** should immediately bring it to the attention of their tutor or one of Greenbank's Named Protection Officers. If at home, then students should initially raise the matter with their parent or guardian, if applicable.
- **Staff** should immediately bring it to the attention of their line manager and/or an SMT member.
- All users should never share personal information over social media and the internet with non-trusted individuals or organisations. This information includes:
  - Phone number
  - Address
  - National Insurance number
  - Birth date
  - Passwords
  - PIN codes
  - Any financial information

- If trusted, then any information should only be sent securely. Students under 18 years old should seek the approval of a parent/guardian.
- Users should recognise that communicating over the internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.

# Cyberbullying

Cyberbullying will not be tolerated. Harassing, 'dissing', flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Do not 'be mean'. Everybody should be treated with dignity and respect. Do not send e-mails, instant messages, or post comments with the intent of scaring, hurting, or intimidating someone else. Similarly, do not circulate photos or video clips of others without their permission.

Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action. In some cases, cyberbullying is a crime. Remember that your activities are monitored and retained by others.

## **Examples of Acceptable Use**

#### You should:

- Follow the same guidelines for respectful, responsible behavior online that is expected to be followed offline.
- Treat social media carefully, and alert your tutor or manager if there is any problem with their usage that would affect your work.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a tutor, Named Protection Officer or SMT member if anything threatening/bullying, inappropriate, or harmful content (images, messages, posts) is seen online that affects Greenbank students or staff.
- Be cautious to protect the safety of oneself and others.

This is not intended to be an exhaustive list. Users should use their own good judgement when using social media.

# **Examples of Unacceptable Use**

#### You should not:

- Use social media in a way that could be personally or physically harmful to oneself or others.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent Greenbank's safety and security measures, and filtering tools.

Use language online that would be unacceptable in a teaching room or office.

This is not intended to be an exhaustive list. Users should use their own good judgement when using social media.

## **Limitation of Liability**

Greenbank will not be responsible for damage or harm to people, files, data, or hardware.

## **Violations of this Social Media Policy**

Violations of this policy may have disciplinary repercussions, including:

- Suspension/removal of volunteer privileges at Greenbank
- Removal from positions of leadership within Greenbank
- Suspension and/or exclusion of a student from Greenbank
- Suspension/cancellation of membership from Greenbank (Sports Academy)
- Disciplinary action
- Additional consequences determined by the CEO (Chief Executive Officer)

**Author**: Andy Barton **Document Version**: V7\_AB230925

Agreed by Greenbank Board of Trustees

Dr Alan Irving, Chairman