GFM Social Media Policy

Read in conjunction with GFM Staff Acceptable Use of ICT
and Mobile Device Policy

Approved by:	GFM Executive	Date:	Nov 2023
Maintained by:	L Mulhall	Next review	Nov 2025

1 About this Policy

The policy has been developed having regard to guidance provided by the professional associations for teachers and school leaders and recognised trade unions. It sets out the rules and standards to be applied for use of the Internet and social media in the GFM. It provides information and guidance for both professional and personal use and outlines the risks to users, as well as the potential consequences of misuse of the Internet and social media.

To reduce repetition of "students or pupils" students has been used throughout and refers to all learners within GFM schools, and so when reading the document substitute pupils where appropriate.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of Social Media may become a matter for police or social care investigations. Staff should also be familiar with Section 5 of the GFM ICT Policy which details personal use of Social Media.

2 Introduction

It is recognised that social networking has the potential to play an important part in many aspects of educational life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

The Internet provides an increasing range of social media tools that allow users to interact with each other. Whilst recognising the important benefits of these media for new opportunities for communication, this policy sets out the principles that GFM staff, governors and contractors are required to follow when using social media.

It is essential that students, parents and the public at large have confidence in the GFM's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that the confidentiality of students and staff members and the reputation of the GFM are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

3 Objectives

The primary objective of this policy is to set out the responsibilities of staff, governors and contractors at the GFM who use the Internet and social networking sites. It is also aimed at ensuring that the Internet and social media are utilised safely, lawfully and effectively for the successful and economic delivery of school-based services.

4 Scope

This policy applies to all teaching and other staff, whether employed by GFM, external contractors providing services on behalf of the GFM, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the GFM. These individuals are collectively referred to in this policy as staff or staff members.

The policy covers personal use of social media as well as the use of social media for official GFM purposes, including sites hosted and maintained on behalf of the GFM. It is acknowledged that there is significant potential for the GFM to exploit the Internet and social media and that this can bring great advantages. The use of both the Internet and social media is therefore actively encouraged.

The policy applies to personal webspace such as social networking sites (for example Facebook, What's App, Instagram, X, LinkedIn), blogs, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia and content sharing sites such as YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

This policy provides a structured approach to using the Internet and social media and will ensure that it is effective, lawful and does not compromise the GFM's reputation, GFM information or computer systems/networks.

5 Risks

The GFM recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the GFM, its staff and the people it serves. Principal amongst these risks are:

- cyberbullying by students;
- access to inappropriate material;
- offending behaviour toward staff members by other staff or students;
- other misuse by staff including inappropriate personal use;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- virus or other malware (malicious software) infection from infected sites;
- disclosure of confidential information;
- damage to the reputation of the GFM;
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;
- civil or criminal action relating to breaches of legislation;
- staff members openly identifying themselves as GFM personnel and making disparaging remarks about the GFM and/or its policies, about other staff members, students or other people associated with the GFM.

6 Applying the Policy

6.1 Responsibilities of staff members

The following principles apply to online participation and set out the standards of behaviour expected of staff members as representatives of the GFM.

The GFM has a duty to provide a safe working environment free from bullying and harassment. If a staff member uses any information and/or communications technology, including email and social networking sites, to make reference to people working at or for the GFM, or people receiving services from the GFM then any information posted must comply with all relevant professional Codes of Practice and the GFM ICT Policy.

6.2 Using the Internet and social media for approved GFM purposes

Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise GFM information or computer systems and networks. They must ensure that their use will not adversely affect the GFM or its business, nor be damaging to the GFM's reputation and credibility or otherwise violate any GFM policies. In particular:

- the GFM’s Internet connection is for business use and its use, and use of social networking, must only take place in line with the GFM’s policies;
- when acting on behalf of the GFM staff must identify themselves as GFM staff when posting;
- personal email or social media accounts must never be used to conduct GFM business. Any accounts created for this purpose must link to a GFM email address. The only exception is the use of professional networks (such as LinkedIn), where it is acceptable to use an account linked to a personal email address in both a professional and personal capacity;
- staff members must report any safeguarding issues they become aware of;
- staff members must not cite or reference students/parents without approval;
- material published must not risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature;
- material published must be truthful, objective, legal, decent and honest;
- material published must not breach copyright;
- any publication must comply with all of the requirements of the Data Protection Act 2018 and GDPR, and must not breach any common law

duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information;

- material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party;
- material published must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;
- the tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner;
- publication must be in line with GFM policies;
- if used with students, staff must ensure that the site's rules and regulations allow the age group to have accounts and that the parents are informed of its use;
- staff members must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the GFM, its staff or services or where they do not have the approval from the School Leadership Team.

6.3 Personal use of Internet and social media

The GFM's Internet connection is intended primarily for educational use. There is no right for staff to use the Internet for private use and access can be withdrawn at any time. Where staff members are permitted access via the GFM's Internet connection:

- the GFM is not liable for any financial or material loss to an individual user in accessing the Internet for personal use;
- staff wishing to spend significant time outside of their own normal working hours using the Internet – e.g. for study purposes must obtain prior approval;
- inappropriate or excessive use may result in disciplinary action and/or removal of Internet facilities;
- the GFM will monitor Internet and email use by electronic means, and staff cannot expect privacy when using the GFM's Internet facility;
- electronic correspondence will only be intercepted in exceptional circumstances.
- users are not permitted to access, display or download from Internet sites that hold offensive material. Offensive material includes, but is not restricted to, hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The GFM is the final arbiter on what is or is not offensive material or what is or is not acceptable, permissible or excessive use of the Internet – staff

concerned about this should refrain from using the Internet for private matters;

- certain websites will be blocked, but it is a breach of this guide to access any of the following types of site unless they are related to researching or preparing class resources that form part of the curriculum):
    - pornography/Adult /mature content
    - gambling/betting/gaming
    - alcohol/Tobacco
    - illegal drugs
    - auction sites
    - violence/hate/racism
    - weapons
    - any site engaging in or encouraging illegal activity
    - illegal file-sharing sites

- staff members who accidentally or unintentionally access a site containing any prohibited content must leave the site immediately and inform the School Leadership Team. Genuine mistakes and accidents will not be treated as breach of this policy;
- staff members may not download software from any source without approval;
- staff members are not permitted to alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures unless they have been given express permission to do so by the Appropriate Line-Manager;
- staff members must not communicate personal or confidential information via the Internet/Intranet for any purpose, unless expressly authorised to do so by their School Leadership Team;
- users must not create, download, upload or transmit any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- users must not create, download, upload or transmit any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material;
- users must not create, download, upload or transmit material that is designed or would be likely to annoy, harass, bully, inconvenience or cause anxiety to others;
- users must not create, download, upload or transmit any unsolicited commercial or bulk web mail, chain letters or advertisements;
- users must not download any digital media including music, images, photos and video that would be in breach of copyright or licensing arrangements, or where copyright or ownership cannot be determined;

- the use of file sharing services or software is prohibited for any purpose;
- the use of personal cloud storage e.g. Google Drive, Dropbox, OneDrive, iCloud, is not permitted for the storage of student or staff sensitive personal data.

6.4 Professional use of Social Media (classroom and beyond the classroom use)

There are many legitimate used of social media within the curriculum and to support student learning. For example, the School and many departments have Facebook/Instagram/ X accounts for the purposes of communicating events and activities within the school. The are also many possibilities for using social media to enhance and develop students' learning.

There must be a strong pedagogical or business reason for creating official school social media account or site. Staff must not create sites unnecessarily or for trivial reasons which could expose the school or GFM to unwelcome publicity or cause reputational damage. As a guideline, we would expect accounts to be limited to one "department" account and one individual staff member account per social media provider. Staff should remember that the greater the number of accounts the greater the risk to the School or GFM of those accounts being "hacked".

When using social media for educational purposes, the following practices must be observed:

- Staff should set up distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and ideally should be linked to an official school email account
- Any new sites should be discussed with the head of department and also the IT team: IT Helpdesk <ithelpdesk@GFM.org>
- The URL, and identity, usernames and passwords of the site should be sent to the IT team: Dan Willis dwillis@bayhouse.GFM.org
- The contend of any school sanctioned social media site should be solely professional and should reflect well on the school and GFM
- **Staff must ensure that the school has parent/carer consent to use, post or publish a photograph or video image of the student.**
- **Staff must ensure that they do not identity a student using their full name. Only first/forename or initials may be used**
- Care must be taken that any links to external sites from the account are appropriate and safe

- Any inappropriate comments or abuse of the school or GFM sanction social media should be immediately removed and reported to a member of the senior leadership team
- Staff should not engage with any direct messaging of students through social media where the message is not public (with the exception of whole school systems e.g. gMail, Google Classroom, Show My Homework)
- Staff should not seek to view/link up with students accounts. For example, in the case of X, staff should not “follow back” those who follow, share or like the comments / posts.

Failure to follow the rules set out in section 6.4 may give rise to disciplinary action.

6.5 GFM reputation and confidentiality

The GFM recognises an employee’s right to a private life. However the GFM must also ensure its reputation and confidentiality are protected. Therefore an employee using any ICT away from GFM, including email and social networking sites must:

- refrain from identifying themselves as working for the GFM in a way that could have the effect of bringing the GFM into disrepute
- not express a personal view as a GFM employee that the GFM would not want to be associated with
- notify the School Leadership Team immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the GFM
- under no circumstances should any GFM staff have any students or any ex-students under the age of 18 as friends on their personal social networking sites. GFM staff are strongly advised not to have any online friendships with any young people (i.e. including those at other schools) under the age of 18, unless they are family members
- exercise caution when having contact or accepting ‘friend’ requests through social media with parents so as not to compromise the GFM’s reputation or GFM information
- not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the GFM and/or partner organisations, students or parents

- not disclose any data or information about the GFM, colleagues in the GFM and/or partner organisations, students or parents that could breach the Data Protection Act 2018 or GDPR regulations
- not use the Internet or social media in or outside of work to bully or harass other staff or others

6.6 Personal Information

GFM staff must never give out personal details of others, such as home address and telephone numbers. Staff must handle all personal or sensitive information in line with the GFM's Data Protection Policies.

With the rise in identity theft and fraud, staff may wish to consider the amount of personal information that they display on personal profiles.

7 Cyber bullying and Harassment

7.1 The use of ICT in relation to Bullying and Harassment

Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim(s) is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

The GFM will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the GFM or in partner organisations, or students or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the GFM or partner organisations, students or parents, can find its way into the public domain even when not intended.

It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

If a staff member receives any threats, abuse or harassment from members of the public through their use of social media then they must report such incidents using the GFM's procedures.

7.2 School Leadership responsibility in relation to Bullying and Harassment

The GFM owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment.

For this reason, it is essential that the School Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, X, or by any other means.

If a School Leader is made aware of such an allegation, the School Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with GFM policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

School Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the School Leadership team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances, the Police should be contacted immediately for advice.

Appendix 1 - Legal and Policy Framework

The GFM is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the GFM are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional Codes of Conduct, including the following:

- Human Rights Act 1998
- Common law duty of confidentiality
- Data Protection Act 2018 and General Data Protection Regulation (2018)
- Employment Practices Data Protection Code

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998 and General Data Protection Regulation (2018)
- Information divulged in the expectation of confidentiality
- GFM or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952, 1996 and 2013
- Copyright, Designs and Patents Act 1988.
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Equality Act 2010