Social Media and Networking Policy 2024

Introduction:

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new, relevant and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with duties to the school, the community, our legal responsibilities and our reputation.

The use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide a balance to support innovation whilst providing a framework of good practice. They apply to all members of staff and students.

- This policy is to ensure clarity of use and guidance for staff, students and all users regarding the use of social media and networking applications.
- This policy is designed to protect individual members of staff, students and all users.
- This policy applies to the use of social media for both business and personal purposes, whether during school/working hours or otherwise.
- This policy applies regardless of whether the social media is accessed using school IT facilities and equipment or equipment belonging to members of staff, students or any other IT/internet enabled equipment.
- Anyone setting up a social media account that is directly connected to Hope Tree School (using the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way) must follow all the guidelines in this policy.
- All staff and students must read, understand and sign the Hope Tree School Online Safety and Acceptable Use Policy.

Purpose:

The purpose of the policy is to:
- Safeguard all pupils and promote wellbeing
- Ensure users are not exposed to risk as a result of their actions
- Use social media in a respectful, positive and productive way which respects all parties involved
- Ensure that the reputation of Hope Tree School (the school), its staff and members of the Advisory Board are protected and that stakeholders understand their ambassadorial role with regard to the school
- Protect the school from legal risks
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the school.

The school defines social media as 'any websites and applications that enable users to create and share content or to participate in social networking'.

- Social networking sites and tools include, but are not limited to, Facebook, Twitter, Snapchat, TikTok, LinkedIn, MySpace, Flickr, YouTube and Instagram.
- It also includes forums and discussion boards such as Yahoo! Groups or Google Groups, online encyclopaedias such as Wikipedia, and any other web sites which allow individual users or organisations to use simple publishing tools.
- Many of the principles of this policy also apply to other types of online presence such as virtual worlds.
- All members of the school community should bear in mind that information they share through social networking applications, even if they are using private spaces, may be subject to copyright, safeguarding and data protection legislation.
- All members of the school community must also operate in line with the school's Equality, Safeguarding and Child Protection, Safer Recruitment and Online Safety and Acceptable Use policies.

School-sanctioned use of social media and/or social media accounts using the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way:

There are many legitimate uses of social media within the curriculum, and to support student learning and to share news with the wider Hope Tree School community. For example, the School has official Twitter, Instagram and Facebook accounts.

There are also many possibilities for using social media to enhance and develop students' learning and to keep the Hope Tree School Community and our supporters in touch with the School.

When using school social media accounts and/or social media accounts using the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way, the following practices must be observed:

- A distinct and dedicated social media site or account will be set up by the school.
- This will be entirely separate from any personal social media accounts held and should be linked to an official school email account.
- Social media accounts must have a link to the Online Safety and Acceptable Use Policy, have official Hope Tree School branding and state that it is an 'Official Hope Tree School Approved Site'.
- If a social media account is identified (that uses the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way) that is not an official Hope Tree School approved site, this should be reported to the Head of Learning.

The social media account must be approved by the Online Safety Officer and updates to passwords must be shared with relevant senior staff.

The content of any School-sanctioned social media site and/or social media accounts using the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way, should be entirely professional and should reflect well on the School.

Staff must not publish photographs of students without the written consent of parents/carers, or the student themselves if they are deemed of the age and ability to provide their own consent.

Standard practice is to publish only the first name and initial of surname, unless permission has been given by parents or students (if deemed of the age and ability to provide their own consent) for the full name to be used.

School sanctioned social media sites must use images of students in suitable clothing.

Staff must take into account the Safeguarding and Child Protection Policy alongside the Staff Behaviour Policy when making any posts on school social media accounts.

Any links to external sites from the accounts must be appropriate and safe; if they are shared these must be verified as reputable sites. Only appropriate hashtags should ever be used.

Any inappropriate comments on, or abuse of, school-sanctioned social media and/or social media accounts using the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way, should immediately be removed and reported to the Online Safety Coordinator and the Designated Safeguarding Lead (DSL).

It is the responsibility of everyone using the site and social media in general to report abuse immediately.

All school sanctioned social media accounts created for school purposes should include a link in the About or Info page to the Online Safety and ICT Acceptable Use Policy on the School website. This will indicate that the account is officially sanctioned by the School.

Use of social media in practice for staff - for personal and professional use:

Staff must not have 1:1 communication, including direct messaging (DM), with students through any social media, apart from via school email accounts.

Google Meet hangouts via a school account and school mobile devices for text messaging. 1:1 communication via Google Meet as part of the Schools Online Learning, must follow the School's Online Safety and Acceptable Use Policy.

Staff should not request or accept any current student of the school of any age or any ex-student of the School under the age of 18 as a friend, follower, subscriber or similar on any personal social media account unless they are the parent of the student or a close family member.

It is advisable that staff do not have contact with previous students (above school age). Staff may remain in communication with past students via a school email account or the School social media accounts.

Any communication received from current pupils on any personal social media sites must be reported immediately to the DSL and to the Online Safety Coordinator.

If any member of staff is aware of any inappropriate communications involving any student in any social media, these must immediately be reported to the DSLs and to the Online Safety Coordinator.

Members of staff must ensure that, wherever possible, and where the social media site allows, their privacy settings on social media sites are set so that students cannot access information relating to their personal lives or follow them on their personal accounts.

All email communication between staff and students of the School on school-related matters must be made from an official school email account (any deviation from this in an emergency must at once be reported to the Head of Learning).

Staff should not use personal email accounts or personal mobile phones to make contact with students of the School, nor should any such contact be accepted.

Staff should not post or publish on the internet or on any social networking site, any reference to the School, their colleagues, parents or students or discuss students or colleagues or criticise the School or staff.

Staff may like, share or make appropriate comments in response to the School's official social media accounts, in accordance with the requirements of this policy.

Staff must not post images on any unofficial Hope Tree School social media account that includes students, unless sharing posts made from a School official social media account.

Staff are instructed to consider the reputation of the School in any posts or comments related to the School on any social media accounts. Reputational breaches by staff are dealt with via the Policy for Appraising Teacher Performance and the Staff Code of Conduct.

Members of staff are responsible for overseeing and monitoring any social media account attributed to their area of responsibility where the social media account is using the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way.

Guidance and advice for staff:

Most common social networking sites are inherently insecure places to have discussions which contain any sensitive information. Privacy laws can be violated and the reputation of the school can be damaged if the public sees a discussion of any sensitive information taking place on social networking. Staff should be aware that these types of cases can result in disciplinary action.

Proprietary Information:

Staff may not share information which is confidential and proprietary about the School. This includes information about services, programmes, financial, strategy, and any other internal confidential, proprietary, or sensitive workplace information that has not been publicly released by the School.

These are given as examples only and do not cover the range of what the School considers confidential and proprietary. If staff have any questions about whether information is proprietary, they must speak to their Line Manager or the Head of Learning before releasing it.

Staff must also be aware of the points made within their employment contract when they joined the School. The School's logo may not be used without explicit permission in writing from the Head of Learning; the School owns the rights to all logos, mottos and phraseology and their usage.

Workplace Privacy:

The School respects staff member rights to privacy and to express themselves. However, the School and staff members must also respect, and diligently protect, the privacy of fellow staff members, students, parents, and others.

Privacy and confidentiality must be maintained in every possible way. Staff must not discuss student or family related information via social networking and public social media, texting, or online unless it is an approved medium and for a school related purpose.

Staff are advised to be extremely cautious in conversations with other staff, parents and volunteers in social networking, on the basis that privacy laws can be violated even if a person's name is not shared.

The School will honour the privacy rights of current and past employees, current and past students and their families, and anyone else associated with the School, by seeking permission before writing about or displaying internal school happenings which might be considered to be a breach of their privacy and confidentiality.

Privacy and Security Settings:

The School recommends staff use security and privacy settings provided by social networking sites.

Regardless of privacy settings, staff are advised to be respectful and responsible in all activity if it in any way involves or references the School, job, or those staff work with.

Staff must understand that on-line content is difficult, if not impossible to retract once posted or sent.

Blogging and Websites:

If staff are developing a website or writing a blog that will mention school staff, the Advisory Board, students, parents/carers and volunteers, they MUST get permission first before writing anything, and advise the Head of Learning they are intending to do this.

The Head of Learning may choose to inspect this from time to time. It is important that staff make appropriate decisions about work-related blogging and the content of blogs, personal websites, postings on wikis and other interactive sites.

Staff are advised to use caution with postings on video or picture-sharing sites, or in comments made elsewhere on the public internet and in responding to comments from posters either publicly or via email.

Where staff are assisting students to develop a website or blog, this must first be approved by the Head of Learning and the Head of Learning must be given password access.

Legal Liability:

Staff should recognise that there is the possibility of being legally liable for something inappropriate which is shared online.

The Media:

If a member of the media or non-traditional online media (including bloggers) contacts a member of staff about the business of the School (e.g.programmes, services, students, parents, policies, practices, or additional business information of any kind), the individual must contact the Head of Learning prior to responding.

Use of social media in practice for students:

Students' use of social media on any school IT systems, School Managed computers and School IT (Google) accounts accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other internet enabled device) brought on to the School site or at a School activity, must comply with the School's Online Safety and Acceptable Use Policy.

Students should also follow any additional code of conduct/guidelines put in place for online learning from home.

Students must not access any social media that is for adults only or if the student does not meet the minimum age requirement.

Anonymous sites must not be accessed as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.

Bad, including offensive, explicit or abusive, language and inappropriate pictures must never be included in messages.

All messages should be positive and not include anything that could be upsetting or defamatory towards others or the School.

Students must take responsibility for keeping details of their accounts private, using full privacy settings and logging off properly and not allowing others to use their accounts.

Students must report anything offensive or upsetting that they see online to the appropriate bodies, either by using the "report abuse" tabs or by speaking to their parents or a member of staff.

It is a serious offence to use another person's account, or to create an account in another person's name without their consent.

Students should not regard anything posted online as private and should remember that harassment, defamatory attitudes and racism are just some issues which could lead to prosecution.

An individual's "Digital Footprint" is becoming increasingly significant when it comes to job and university applications. If unfortunate decisions are made, it will be extremely difficult, perhaps impossible, to eliminate the evidence.

If students see inappropriate postings by other students, they must inform the school so that steps can be taken to avoid possible repercussions.

The Malicious Communications Act applies to social media interaction by students, Staff and Parents of the School.

Students must have permission from the Head of Learning for any social media accounts using the name of Hope Tree School, a Hope Tree School logo, or clearly attached to Hope Tree School in some way.

Use of social media in practice for parents:

- Positive contributions to the School Social Media are welcomed.
- Any concerns or issues about the School, its students or staff should be expressed directly to the School and not be voiced on social media.
- Parents must obtain permission before posting pictures that contain other parents or their children, unless sharing or liking a post from the School's official social media account.
- If parents become aware of inappropriate use of social media by their own or other people's children, they should contact the School so that the School can work with the parents to educate young people on safe and appropriate behaviour.
- If parents become aware of the inappropriate use of social media by other parents or school staff, they should inform the School so that steps can be taken to remedy the situation.

Further Guidance:

Further guidance on educating and safeguarding young people online and responding to incidents:
Sexting UK Council for Child Internet Safety Guidance - Sexting
Online safety advice for pupils, parents and teachers:
www.thinkuknow.co.uk
http://www.saferinternet.org.uk/
https://www.internetmatters.org/ Cyberbullying
www.childnet.com/cyberbullying-guidance
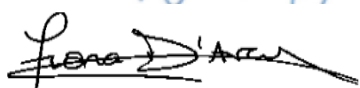Preventing radicalisation educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
https://www.internetmatters.org/resources/what-age-can-my-child-start-socialnetworking/

Signed: *[signature]*   Head of Learning

          [signature]   Head of Pastoral Care

Date: March 2024   Review Date: March 2025