Felsted

SOCIAL MEDIA POLICY

BOTH SCHOOLS INCLUDING EYFS AND BOARDING

Governors' Committee normally reviewing:	Governance Committee
Date last formally approved by the Governors :	Summer Term 2022
Date became effective :	May 2015

Period of Review:	Annually
Next Review Date :	Summer Term 2023

Person responsible for implementation and monitoring :	Designated Safeguarding Lead (Prep and Senior School)
Other relevant policies :	Safeguarding (Child Protection and Staff Behaviour) Policy Anti-Bullying Policy Equal Opportunities Policy Sex and Relationship Education Policy Safer Recruitment Policy Equal Opportunities Policy Online Safety ICT Acceptable Use Policy

The following Policy encompasses the Aims and Ethos of the Preparatory School and the Senior School

Aims and Ethos

SAFEGUARDING STATEMENT
Felsted is committed to maintaining a safe and secure environment for all pupils and a 'culture of vigilance' to safeguard and protect all in its care, and to all aspects of its 'Safeguarding (Child Protection and Staff Behaviour) Policy'.

EQUAL OPPORTUNITIES STATEMENT
The aims of the School and the principles of excellent pastoral care will be applied to all children irrespective of their race, sex, disability, religion or belief, sexual orientation, gender reassignment or pregnancy or maternity; equally these characteristics will be recognised and respected, and the School will aim to provide a positive culture of tolerance, equality and mutual respect.

SOCIAL MEDIA AND NETWORKING POLICY

1. Policy Statement

To ensure clarity of use and guidance for staff, pupils and all users regarding the use of social media and networking applications.

This policy is designed to protect individual members of staff, pupils 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, pupils or any other IT/internet enabled equipment.

Anyone setting up a social media account that is directly connected to Felsted School (using the name of Felsted School, a Felsted School logo, or clearly attached to Felsted School in some way) must follow all the guidelines in this policy.

All staff and pupils must read and understand the Online Safety and ICT Acceptable Use Policy and sign / accept the Staff Computer / Device Agreement and Code of Conduct for ICT.

2. Rationale

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 School 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 this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff and pupils.

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 Felsted School (the School), its staff and governors is 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.

3. Definitions and Scope

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, 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 should bear in mind that information they share through social networking applications, even if they are on private spaces, may be subject to copyright, safeguarding and data protection legislation. They must also operate in line with the School's Equalities, Harassment, Child Protection, Safer Recruitment and Online Safety and ICT Acceptable Use policies.

4. School-sanctioned use of social media and/or social media accounts using the name of Felsted School, a Felsted School logo, or clearly attached to Felsted 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 Felsted School community. For example, the School and sub-departments of the School have official Twitter, Instagram, Facebook, LinkedIn and TikTok accounts and several A-level courses require the use of blogs for assessment. There are also many possibilities for using social media to enhance and develop pupils' learning and to keep the Felsted 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 Felsted School, a Felsted School logo, or clearly attached to Felsted School in some way, the following practices must be observed:

4.1. A distinct and dedicated social media site or account must be set up by the Marketing Department. This should 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 ICT Acceptable Use Policy, have official Felsted branding by the Marketing Department and state that it is an 'Official Felsted School Approved Site'. If a social media account is identified (that uses the name of Felsted School, a Felsted School logo, or clearly attached to Felsted School in some way) that is not an official Felsted School approved site, this should be reported to the Marketing Department.

4.2. The social media account must be approved by the appropriate Head or SLT/LT member and updates to passwords must be shared with the Marketing Department.

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

4.4. Staff must not publish photographs of pupils without the written consent of parents / carers, or the pupil 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 pupils (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 children in suitable clothing.

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

4.6. 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.

4.7. Any inappropriate comments on, or abuse of, school-sanctioned social media and/or social media accounts using the name of Felsted School, a Felsted School logo, or clearly attached to Felsted School in some way, should immediately be removed and reported to the E-safety Officer, Designated Safeguarding Lead (DSL) and the Marketing Department (if appropriate). It is the responsibility of everyone using the site and social media in general to report abuse immediately.

4.8. 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.

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

5.1. Staff must not have 1:1 communication, including direct messaging (DM), with pupils 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 Learning: Policy and Procedures for Teaching Staff.

5.2. 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 pupil or a close family member.

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

5.4. Upper Sixth pupils are invited to join The Felsted Network, that staff are also members of, following the leavers' briefing.

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

5.6. 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.

5.7. 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 pupils cannot access information relating to their personal lives or follow them on their personal accounts.

5.8. All email communication between staff and pupils of the School on school business must be made from an official school email account (any deviation from this in an emergency must at once be reported to the line manager). Staff should not use personal email accounts or personal mobile phones to contact pupils of the School, nor should any such contact be accepted, except in circumstances such as school trips or away matches that have been given prior approval by the Heads (Prep or the Senior School). Prior approval may also be given by the Head of the Senior School for staff to communicate professionally with pupils on School premises for safety reasons.

5.9. Staff should not post or publish on the internet or on any social networking site, any reference to the School, their colleagues, parents or pupils or discuss pupils or colleagues or criticise the School or staff. Staff may like, share or make appropriate comment in response to the School's official social media accounts, in accordance with Section 4.

5.10. Staff must not post images on any unofficial Felsted social media account that includes pupils, unless sharing posts made from a School official social media account.

5.11. 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 Disciplinary Policy.

5.12. 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 Felsted School, a Felsted School logo, or clearly attached to Felsted School in some way.

6. 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 our 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 SLT/LT member before releasing it. Staff must also be aware of the points made within their employment contract when they joined the School, a copy which can be obtained from HR.

The School’s logo and mascots may not be used without explicit permission in writing from the Marketing Department; the School owns the rights to all logos, mascots, 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, pupils, parents, and others. Privacy and confidentiality must be maintained in every possible way.

Staff must not discuss pupil 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 pupils 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 the School and/or our Common Room, staff, Governors, pupils, parents and volunteers, they MUST get permission first before writing anything, and advise the Headmaster they are intending to do this. The Head 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. If staff are assisting pupils to develop a website or blog, this must first be approved by the Head/SLT/LT member and the Head /SLT/LT member 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, pupils, parents, clubs, policies, practices, or additional business information of any kind), the individual must contact the Marketing Department prior to responding.

7. Use of social media in practice for pupils

7.1. Pupils use of social media on any School IT systems, School Managed Chromebooks 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 Pupils' Computer/Device Usage Agreement and the School's Online Safety and ICT Acceptable Use Policy. Pupils should also follow any additional code of conduct / guidelines put in place for online learning from home.

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

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

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

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

7.6. Pupils 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.

7.7. Pupils 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.

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

7.9. Pupils 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.

7.10. 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.

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

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

7.13. The age restrictions for social media platforms” link (see further guidance) is used as a visual aid for pupils around the School. It demonstrates the ages at which children are allowed to access various Social Media platforms, as well as serving as a starting point for discussion about the safe use of Social Media. It is referred to during ICT and Computer Science lessons, as well as eSafety lessons and Assemblies.

7.14. Within Hamilton House (the Prep School Boarding House) any social media sites on personal devices must be sanctioned and monitored by parents and fall within the relevant age restriction. Boarders in Hamilton House are not permitted to access any social media platforms which are not age appropriate whilst boarding. If there is evidence of access then the Schools Behaviour and Discipline Policy will be followed.

7.15. Pupils must have permission from the relevant HM or Head of Department for any social media accounts using the name of Felsted School, a Felsted School logo, or clearly attached to Felsted School in some way

8. Use of social media in practice for parents

8.1. Positive contributions to the School Social Media, such as Twitter, are welcomed.

8.2. Any concerns or issues about the School, its pupils or staff should be expressed directly to the School and not be voiced on social media.

8.3. 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.

8.4. 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.

8.5. 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

Social Media Restrictions for Social Media Platforms

What are the age limits for social media apps and platforms?

It is vital that parents, pupils and staff know the age restrictions that are applied to many popular apps. As this is a fast moving area we would recommend that parents (with their child) always check before a child accesses an app from an internet safety website such as Internet Matters, for which there is a link below. We do not endorse the use of these apps; this information is provided only to help support your children to use social media safely.
https://www.internetmatters.org/resources/what-age-can-my-child-start-social-networking/