Social Media Policy

This policy has been developed to provide rules and standards which are to be applied for use of the Internet, with a specific focus on Social Media use in Heathfield School and use by employees of Heathfield School.
This policy applies to all staff, teaching and non-teaching employed by Hampshire County Council, the school governing body and external contractors providing services on behalf of the school, this also includes volunteers.
Information has been taken from Hampshire County Council's recommendations for School Social Media Policy.

Introduction:

Social media and social networking plays a significant part in many aspects of our lives, including teaching & learning; external communications and continuing professional development.

The purpose of this policy is to encourage the responsible and professional use of social media. There is an ever increasing range of social media tools that enable users to interact with each other, and whilst this has many benefits there are principles that school staff, governors and contractors are required to follow when using social media.

The main principle of this policy is ensure that staff members use social media responsibly so that confidentiality of students, staff members and the reputation of the school and Hampshire County Council are safeguarded. It is crucial that staff members are conscious and responsible for keeping their personal and professional lives separate.

Every staff member and Governor at Heathfield School have a responsibility to use the Internet and social media safely, lawfully and effectively.

This policy should be referred to in conjunction with the Heathfield Computing Policy and Heathfield E-Safety Policy. This policy covers the personal use of social media as well as the use of social media for official school purposed, including sites hosted and maintained on behalf of the school.

Risks:

Heathfield recognises that there are risks associated with the Internet and the use of social media, and takes steps to regulate their use to ensure this does not damage the school, its staff and its reputation.

Such risks include:

- Cyber bullying by pupils / students and staff
- Access to inappropriate material (see also Safeguarding Policy)
- Offending behaviour toward staff members by other staff and / or pupils / 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 infection from infected sites
- Disclosure of confidential information
- Damage to the reputation of the school
- Social engineering attacks (e.g. 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 school personnel and making disparaging remarks about the school and / or its policies, about other staff members, pupils or other people associated with the school

Responsibilities of staff members

The school has a duty to provide a safe working environment free from bullying and harassment. Any use of communication technology, including email and social networking sites, by a staff member making reference to people working at or for the school must adhere to all relevant Codes of Practice and the School's ICT Acceptable Use Policy.

Personal use of the Internet and Social Media

The school's Internet connection is intended primarily for educational use. Staff do not have a right to use the Internet for private use and access can be withdrawn at any time.

Staff members should be aware that where they are permitted to access via the school's Internet connection:

- The school is not liable for any financial or material loss to an individual user accessing the Internet for personal use
- Inappropriate or excessive use may result in disciplinary action and / or removal of Internet facilities
- The school will monitor Internet and email use by electronic means, and staff should not expect privacy when using the school's Internet facilities
- Personal (e.g. your login to the server) Internet use, search histories and the content of emails sent for personal use may be accessed by staff only

according to the Council's Internet, Intranet and Email Monitoring Policy and School's disciplinary procedures. This would occur only when a legitimate concern has been raised by monitoring processes, legitimate concerns expressed by colleague, or some other legitimate and objective complaint or incident

- 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 materials include, and are not restricted to, hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The school is the final arbiter on what is and is not deemed to be offensive material or what is or is not acceptable, permissible or excessive use of the Internet. If you have any concerns regarding this, then you are advised to refrain from using the Internet for private matters
- The use of streaming media such as video (YouTube; BBC iPlayer; Vimeo, etc.) or audio (internet radio, Spotify, Google Music, etc.) should be kept to a minimum. Streaming should be limited to occasional short video / audio clips only. TV, films, continual broadcasts (e.g. news, sport, radio etc.) should NOT be streamed.
- Downloading of media for personal use such as video (YouTube; BBC iPlayer; Vimeo, etc.) or audio (internet radio, Spotify, Google Music, etc.) is not permitted.
- Websites deemed inappropriate for use by staff, and pupils, will be blocked. Staff are not permitted to access the following types of site:
    - 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
- Any access by school staff, accidentally or unintentionally, to a site containing any prohibited content must leave the site immediately and report it to the Senior Leadership Team and the Computing Team who will make a decision about whether the site needs to be blocked. Genuine mistakes will not be treated as a breach to this policy.
- It is not permitted for staff members to download software from any source without approval from the Computing Team
- 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 Headteacher or Computing Team (this includes use with the pupils)
- Obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material must not be created, downloaded, uploaded or transmitted by any user

- Material that is designed or would be likely to annoy, harass, bully, inconvenience or cause anxiety to others must not be created, downloaded, uploaded or transmitted by any user
- Unsolicited commercial or bulk webmail, chain letters or advertisements must not be created, downloaded, uploaded or transmitted by any user
- 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 must not be downloaded by users
- The use of file sharing services or software is prohibited for any purpose
- The use of 'cloud' storage (e.g. Google Drive; Dropbox; SkyDrive; iCloud) is not permitted for the storage of sensitive personal data

Approved School Purposes:

Staff must be aware that:

- The school's Internet connection if for business purposes and the use of social networking must not take place
- Personal email or social media must never be used to conduct school business. Any accounts created for this purpose MUST link to a school email address. The only exception is the use of professional networks (such as LinkedIn) where it is acceptable to link a personal email for both a professional and personal capacity
- Staff are responsible for reporting any safeguarding issues they become aware of
- Staff members must not cite or reference pupils / students / parents without approval
- Material published must not risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature (see also Safeguarding Policy and PREVENT Strategy)
- Material published must be truthful, objective, legal, decent and honest
- Material published must not breach copyright
- Any publication must comply with all the requirements of the Data Protection Act 1998, 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 parts 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 used in any publications must be respectful and professional at all times, and must not be in an abusive, hateful, or otherwise disrespectful manner
- Any publications must be in line with school policies
- Social media must not be used by staff members if doing so could pose as a risk (finically or reputational) to the school, its staff or services where it has not been approved by the Senior Leadership Team

- The Internet and Social Media use with pupils / students must adhere to the school's rules and regulations appropriate to the pupils and parents are informed of its use

School reputation and confidentiality:

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

- Refrain from identifying themselves as working for the school in a way that could have the effect of bringing the school into disrepute
- Not express a personal view as a school employee that the school would not want to be associated with
- Notify the Senior 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 school. This includes, and is without exception, to material published that is of an illegal, sexual, discriminatory or offensive nature (see also Safeguarding Policy)
- Not have any unauthorised contact or accept 'friend' requests through social media with any pupil / student under the age of 18 (or under the age of 19 where the school has such a provision). This includes former pupils / students and / or those who attend other schools) unless they are family members
- Not contact or accept 'friend' requests through social media with any parents or carers. It is important for staff to promote professional relationships with our pupils and their families and to maintain a boundary between their professional and personal lives
- Not allow interaction through information and communications technology, this includes the use of emails or social networking sites, that damages relationships with work colleagues in the school, and / or partner organisations, pupils or parents
- Not disclose any data or information about the school, colleagues in the school or partner organisations, pupils or parents that could breach the Data Protection Act 1998
- Not use the Internet or social media in or outside of work to bully or harass other staff or others

School 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 school's Data Protection Policies.

All staff should be aware of the rise in identity theft and fraud, and should consider the amount of personal information that they display on personal profiles

Cyber bullying and Harassment:

This section of the policy refers to the use of ICT in relation to Bullying and Harassment

It should be noted that Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, implies 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. Therefore bullying and harassment now include the use of information and communications technology (including email and social networking).

The school has a responsibility to consider it a potential disciplinary matter staff are found to be using ICT, including email and social networking sites, in such a way as to bully / harass others in the school or partner organisations, or pupil or parents. This includes both during and outside of work.

It is crucial that all staff members are aware that no matter what the privacy settings on their social media / networking site, inappropriate or derogatory information about a colleague in the school, partner organisations, parents or pupils can find its wat into the public domain event when not intended. The context and content can also be misconstrued.

It should be noted that a person does NOT need to have directly experiences this victimisation for it to be classes as cyber bullying / harassment.

In the event that a staff member receives any threats, abuse or harassment from members of the public through their use of social media, they must report it using the school's procedures. Support is available through Hampshire's confidential counselling service, Employment Support *(0800 030 5182)*

The Senior Leadership Team have a responsibility in relation to Bullying and Harassment.

The school 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 Senior 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 Twitter or by any other means).

If a member of the Senior Leadership Team has been made aware of such an allegation, this should be dealt with in the same way as any other incident of bullying or harassment in line with school policies. If the incident involves illegal content or contains threats of a physical or sexual nature, or any matters of a safeguarding issue arise (see also Safeguarding policy, including the PREVENT Strategy), the Senior 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 the image or show it to anyone else. Evidence, therefore should be kept in a secure location such as a located cupboard where others are not able to access it and the Police should be contacted immediately.

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, dismissal, and / or withdrawal to access to ICT facilities.

Staff should be aware that in certain instances, inappropriate use of Social Media may become a matter for the police or social care investigations.

Staff should read this policy and sign a declaration to confirm that they have had access to the School Social Media Policy and they accept and will follow the terms.

Policy by: Hayley Sae Kang (Computing Co-Ordinator)
Date: June 2017
To be reviewed: June 2018