Tower Hill Primary School
Social Media Policy

Date (reviewed): Summer 2018 **Author: Michaela Corper**
Review Date : Summer 2020 **ICT Leader**

1 Preamble

1.1 This document should be read in conjunction with information contained in the Acceptable Use of ICT Policy and the E-Safety Policy, together with the "Guidance on using Social Media" and other related policy documents referred to at Appendix 1 below.

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

1.3 Where staff have concerns about e-safety, these should be raised with the Headteacher. Advice can also be sought from professional associations and trade unions.

2 Introduction

2.1 It is recognised that social networking has the potential to play an important part in many aspects of school 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.

2.2 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 school staff, governors and contractors are required to follow when using social media.

2.3 It is essential that pupils/students, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and staff members and the reputation of the school and the County Council 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

3.1 The primary objective of this policy is to set out the responsibilities of staff, governors and contractors at the school 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

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

4.2 The policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school. It is acknowledged that there is significant potential for the school 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.

4.3 The policy applies to personal webspace such as social networking sites (for example Facebook, MySpace, Yapper), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and 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.

4.4 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 school's reputation, school information or computer systems/networks.

5 Risks

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

- cyber bullying by pupils/students;
- access to inappropriate material;
- offending behaviour toward staff members by other staff 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 (malicious software) infection from infected sites;
- disclosure of confidential information;

- damage to the reputation of the school;
- 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 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.

6 Applying the Policy

6.1 Responsibilities of staff members

6.1.1 The following principles apply to online participation and set out the standards of behaviour expected of staff members as representatives of Tower Hill Primary School.

6.1.2 Tower Hill Primary School 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 school, or people receiving services from the school then any information posted must comply with all relevant professional Codes of Conduct and Tower Hill's ICT Acceptable Use Policy.

6.2 Using the Internet and social media for approved school purposes

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

- the school's Internet connection is for business use and its use, and use of social networking, must only take place in line with the school's policies;
- when acting with approval on behalf of the school, under no circumstances may staff comment or contribute unless identifying themselves as school staff;
- personal social media accounts 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 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 pupils/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 which is the implementation of the General Data Protection Regulation [GDPR] 2016, 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 school policies;
- if used with pupils/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 school, its staff or services or where they do not have the approval from the Senior Leadership Team.

6.3 Personal use of Internet and social media

6.3.1 The school'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 school's Internet connection:

- the school 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 school will monitor Internet and email use by electronic means, and staff cannot expect privacy when using the school's Internet facility;
- personal Internet search histories and the content of emails sent for personal use will be accessed by staff only according to the Council's Internet, Intranet and Email Monitoring Policy and school's disciplinary procedures, and only then when a legitimate concern has been raised by monitoring processes, legitimate concerns expressed by a 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 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 school 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;

- due to the potential impact on school systems, 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. Staff members must not stream TV, films or continual broadcasts (e.g. sport, news, radio or playlists);
- due to the potential impact on school systems, the 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;
- certain websites will be blocked, but it is a breach of this guide to access any of 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

- staff members who accidentally or unintentionally access a site containing any prohibited content must leave the site immediately and inform the Senior 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 Headteacher;
- staff members must not communicate personal or confidential information via the Internet/Intranet for any purpose, unless expressly authorised to do so by their Senior 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 cloud storage e.g. Google Drive, Dropbox, SkyDrive, iCloud, is not permitted for the storage of sensitive personal data.

6.4 School reputation and confidentiality

6.4.1 The school recognises an employee's right to a private life. However the school must also ensure its reputation and confidentiality are protected. Therefore an 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
- not have any unauthorised contact or accept 'friend' requests through social media with any pupil/student under the age of 18 (or under age 19 where the school has such provision), (including former pupils/students and/or those who attend other schools) 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 school's reputation or school information;
- not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the school and/or partner organisations, pupils/students or parents
- not disclose any data or information about the school, colleagues in the school and/or partner organisations, pupils/students or parents that could breach the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018
- not use the Internet or social media in or outside of work to bully or harass other staff or others.

6.5 Personal Information

6.5.1 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.

6.5.2 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

7.1.1 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.

7.1.2 The school 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 school or in partner organisations, or pupils/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 school or partner organisations, pupils or parents, can find its way into the public domain even when not intended.

7.1.3 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.

7.1.4 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 school's procedures. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182).

7.2 Senior Leadership responsibility in relation to Bullying and Harassment

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

7.2.2 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.

7.2.3 If a Senior Leader is made aware of such an allegation, the Senior Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school 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.

7.2.4 Senior 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 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 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.

8. Signature

8.1 It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the School Social Media Policy and that they accept and will follow its terms.

8.2 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.

Appendix 1

Legal and Policy Framework

Tower Hill Primary School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school 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
- General Data Protection Regulations (GDPR) 2016 and Data Protection Act 2018, and
- Employment Practices Data Protection Code

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the General Data Protection Regulations (GDPR) 2016 and the Data Protection Act 2018
- Information divulged in the expectation of confidentiality
- School or County Council business 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

Related Policies

The Social Media policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- County Council Guidance on using Social Media
- IT Policy on email and internet use
- IT acceptable usage standards
- ICT Acceptable Use Policy for Staff
- Internet and Intranet Monitoring Policy
- Cyber bullying: Practical Advice for School Staff
- Disciplinary Procedures
- Equalities Policy

Appendix 2

Staff Declaration

I have read and understand the School Social Media Policy and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that, in certain circumstances, inappropriate use of Social Media may become a matter for police or social care investigations. I understand that if I need any clarification regarding my use of Social Media, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: …….

DATE: …….

PRINT NAME: ……