Owlswick School and Home

Social Media Policy for Staff

Approved by:	Leon Creenan/Sarah Hawke	**Date:**	29/11/18
Last reviewed on:	29/11/18		
Next review due by:	29/11/19		

Owlswick School and Home Social Media Policy

Introduction

The Internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

While recognising the benefits of these media as new opportunities for communication, this policy sets out the principles that Owlswick staff are expected to follow when using social media.

It is crucial that young people, parents and the public at large have confidence in Owlswick'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 young people, staff and reputation of Owlswick is safeguarded.

Staff members must be conscious at all times of the need to keep their personal and professional lives separate and consider this separation in terms of how they manage their own personal electronic devices, data and social media accounts.

Policy Scope

This policy applies to all members of staff employed to work at Owlswick School and Home.

This policy covers personal use of social media as well as the use of social media for official Owlswick purposes, including any sites that may be hosted and maintained on behalf of Owlswick

This policy applies to personal web space such as social networking sites, for example *Facebook, Whats App, Messenger, Instagram, Tumblr, Snap Chat*, blogs, vlogs, microblogs such as *Twitter*, chatrooms, forums, Podcasts, open access online encyclopaedias such as W*ikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *Flickr* and *YouTube* and decoy apps. 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.

Related Policies

This policy should be read in conjunction with the following Owlswick and policies

- Owlswick School and Home Staff Handbook
- Owlswick School and Home Child Protection and Safeguarding Policy
- Owlswick School and Home E-safety policy
- Owlswick School and Home Anti-Bullying Policy
- Owlswick School and Home Missing Person's Policy
- Owlswick School and Home Tackling Extremism and Radicalisation Policy

Legal Framework

Owlswick is committed to ensuring that all staff members provide confidential services that meet the highest standards.

All individuals working on behalf of Owlswick 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 Human Rights Act 1998
- Common law duty of confidentiality, and
- The Data Protection Act 2018.

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. young people and employee records protected by the Data Protection Act 2018
- Information divulged in the expectation of confidentiality
- Owlswick 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 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

Owlswick could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render Owlswick liable to the injured party.

Safeguarding and Child Protection

Owlswick is committed to ensuring that young people are safeguarded in all aspects of their lives and that individuals can expect to feel safe and be kept safe in their home and school environment.

Safeguarding and child protection covers and is related to a number of areas which relate to the risks of young people being for example:

- Sexually exploited and a victim of child sexual exploitation
- Becoming radicalised
- Going missing

- Becoming involved in gang culture or crime
- Becoming the victims of crime
- Being bullied
- Being victims of sexual violence and harassment between children

All of the above areas can be related to internet safety as the internet and social media are used to groom and exploit young people after gaining their confidence and adults or other young people seeking to form relationships.

All young people have a linked key worker from the care team who will be responsible for completing an E-safety agreement with them for the use of all technological devices within the house. Each young person also completes an E-safety agreement for using computer equipment and software programmes in school.

If an E-safety incident occurs regarding a young person, staff will follow a set procedure and report this incident (using the E-safety incident reporting process) to the Designated Child Protection Lead (DCPL). The DCPL who will make a decision about the immediate action needing to be taken and if the child protection policy needs to be evoked. In the absence of the DCPL, the incident would be reported to the senior manager from home or school for a decision about the action to be taken.

There are strict guidelines set out in the Owlswick E-safety policy regarding how staff monitor the use of the internet and social media by young people in order to ensure they are being safeguarded. Please refer to the E-safety policy.

Owlswick has a software security system that enables Internet sites/programmes to be blocked by the moderators of the system who are the E-safety champions and senior managers. Owlswick's primary aim is to educate young people to feel and be safe when using the internet and social media as well as to enjoy exploring and being able to be creative. However there is a safeguarding requirement to ensure that certain sites are not available to individuals or groups if they search on-line or try to connect to a certain site which may show pornographic images for example. All the safeguarding and monitoring procedures and systems have a reference to the national requirements and regulations on Children's Homes to safeguard young people.

Policy Principles

Staff members need to be professional, responsible and respectful when using social media.

Staff must be conscious at all times of the need to keep their personal and professional lives separate. They should not put themselves in a position where there is a conflict between their work at Owlswick work and personal interests.

Staff must not engage in activities involving social media which might bring Owlswick into disrepute.

Staff must not share information regarding Owlswick's business or any activity connected to Owlswick on any social medium.

Staff must not represent their personal views as those of Owlswick on any social medium.

Staff must not share or discuss personal information about young people and other professionals they interact with as part of their job on social media. They must also not make reference to their day to day work activity at Owlswick or give any details about their roles which identify Owlswick as their place of work as this is a breach of confidentiality.

It is strictly forbidden for individual staff's own personal devices such as mobile phones, lap tops and iPad to be used by a young person.

Staff must on no account use their own personal devices to share, store or show any photographs, personal information or social media accounts to any young person in their care or education. All personal devices that are brought into home or school need to be password protected and kept in a secure place when they are not being used meaning they are not accessible to any young person. No images of /personal information regarding a young person are to be stored on any personal staff devices at work or at home. This forms part of the safeguarding policy and procedure. Failure by individual staff members to adhere to this policy may result in Owlswick taking disciplinary action against the member of staff.

Staff must not use social media to share personal or professional information about a colleague or an activity related to colleagues on any social medium with one another or any young person.

Staff must not use social media and the internet in any way to attack, insult, abuse or defame young people, their family members, colleagues, other professionals, other organisations, and the Owlswick proprietors, managers or Owlswick itself. Staff must not use social media to bring the reputation of Owlswick into disrepute.

Staff must not use social medium to express their discontent about their own role or any aspect about how Owlswick operates. If there are any issues for staff in these areas they must use the appropriate channels to raise them with their line manager or the proprietors.

Staff must be accurate, fair and transparent when creating or altering online sources of information on behalf of Owlswick.

Staff failure to comply with any aspect of the social media policy may result in disciplinary action being taken against them.

Personal Use of Social Media

Staff members must not identify themselves as employees of Owlswick in their personal web space. This is to prevent information on these sites from being linked with the home and school and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services, and young people.

Staff members must not and not permitted to have contact through any personal social medium with any current young person or previous young person who has been on a placement at Owlswick

Staff members must not and are not permitted to have any contact with any current young person's family members through personal social media as that contact are likely to constitute a conflict of interest and may breach professional boundaries and relationships.

If staff members wish to communicate with any current young people through social media sites, they can only do so with the approval of Owlswick, using official Owlswick sites and

accounts created specifically for this purpose. These sites are managed and controlled by Owlswick administrators.

Staff members must decline 'friend requests' from young people they receive in their personal social media accounts. Instead, if they receive such requests from young people, they must discuss these in general terms and signpost young people to become 'friends' of the official Owlswick Facebook account for example.

On leaving Owlswick's service, staff members must not contact young people by means of personal social media sites and will be reported to the administrators of these sites if contact is made.

Information that staff members have access to as part of their employment, including personal information about young people and their family members, colleagues and Owlswick corporate information must not be discussed on their own personal web space.

Photographs, videos or any other types of image of young people and their families or images depicting staff members or the identification of the Owlswick premises must not be published on personal web spaces/social media accounts.

Owlswick staff email addresses and other official contact details must not be used for setting up personal social media accounts, any business accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Owlswick's corporate image must not be used or published on personal web spaces/social media accounts.

Owlswick only permits limited personal use of social media while at work. Access to social media sites for personal reasons is not encouraged and staff are expected to access these sites within their own time. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the Internet should not be on Owlswick's time.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

Staff members must ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Using social media on behalf of Owlswick

Staff members can only use official Owlswick sites for communicating with young people or to enable young people to communicate with one another.

There must be strong pedagogical or business reasons for creating official Owlswick sites to communicate with young people or others. Staff must not create sites for trivial reasons which could expose Owlswick to unwelcome publicity or cause reputational damage.

Any official sites must be created only according to the requirements as agreed with the Proprietors/Registered Manager and Head Teacher and there must be a specific reason why the site is be set up. Permission must be granted and administrators agreed in advance of the site being created. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

At all times staff members must act in the best interests of young people when creating, participating in or contributing content to social media sites.

Monitoring of Internet Use

Owlswick monitors usage of its Internet and email services without prior notification or authorisation from users. Owlswick reserves the right to monitor the official work email accounts and internet usage of staff members.

Users of Owlswick's email and Internet services should have no expectation of privacy in anything they create, store, send or receive using Owlswick's ICT system.

Breaches of the policy

Any breach of any aspects of the above policy may lead to disciplinary action being taken against the staff member/s involved in line with Owlswick's Disciplinary Policy and Procedure. This action may lead to a staff member being dismissed from their employment with immediate effect.

A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Owlswick or any illegal acts or acts that render Owlswick liable to third parties may result in disciplinary action or dismissal.

Contracted providers of Owlswick services must inform the relevant Owlswick manager immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of Owlswick. Any action against breaches should be according to contractors' internal disciplinary procedures.