GLENWOOD SECONDARY SCHOOL, EMSWORTH

USE OF SOCIAL MEDIA POLICY

Reviewed	**February 2018**
Responsibility to Review	**HT**
Next Review	**February 2019**
Approval	**FGB**

This policy should be read in conjunction with other policies including Online Safety Policy, Data Protection and Freedom of Information policies. This Policy was developed using guidance from Create Social Media Guidelines for Your School (Edutiopia / Facebook) and Securus Monitoring.

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 Glenwood School staff are expected to follow when using social media.

It is crucial that young people, parents and the public at large have confidence in Glenwood 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 our young people, staff and the reputation of Glenwood School are safeguarded.

Staff members also must be conscious at all times of the need to keep their personal and professional lives separate.

STATEMENT OF DUTY OF CARE
Glenwood School is committed to ensuring that our young people are safeguarded in all aspects of their lives and that individuals can expect to feel safe and be kept safe in their school environment. This may extend to the young peoples' home environment as well.
Safeguarding and child protection covers and is related to a number of areas, which relate to the risks of young people for example being:

- 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

All of the above areas can be related to online 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 our pupils and staff complete and Acceptable User Agreement, which includes agreeing to use the school's IT facilities in a safe, sustainable manner and to report any issues of concerns to the appropriate person.

SCOPE OF POLICY
This policy applies to all staff that work at Glenwood School. These individuals are collectively referred to as 'staff members' in this policy. This policy applies to all of the young people who receive their

education at Glenwood School. This policy covers personal use of social media as well as the use of social media for official school purposes, including sites that may be hosted and maintained on behalf of Glenwood School.

This policy applies to personal webspace such as social networking sites (for example *Facebook*, *MySpace, Instagram, tumblr, Snap Chat*), blogs, mircoblogs 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*. The Internet is a fast moving technology and it is impossible to cover all circumstances or emerging media therefore the principles set out in this policy must be followed irrespective of advances in technology.

Glenwood School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of Glenwood 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.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media.

Glenwood School could be held responsible for acts of their employees in the course of their employment. For example, staff members who harass colleagues 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 Glenwood School liable to the injured party.

STATEMENT OF TEACHING SAFE PRACTICES

"Children and young people need to be empowered to keep themselves safe - this isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends, but we also teach children how to swim." Byron Report (2008).

Pupils entering Glenwood School, like young people anywhere, are increasingly familiar with mobile technology but often lack the corresponding level of awareness of online safety. It is therefore essential that during their time here they develop an understanding of how to enjoy mobile technologies but at the same time learn how to reduce their vulnerability e.g. by either doing something of their own volition (or through coercion) or unwittingly making information available that unscrupulous people will benefit from etc. Teaching safe practices applies to staff and governors as well as pupils. Whilst online safety is emphasised to pupils on a daily basis, discrete online safety awareness lessons are provided across the whole school with age-appropriate activities during the spring term to coincide with Safer Internet Day. In addition, the school participates in the Internet Cyber Safety programme, run by Hampshire Constabulary.

NETWORK PROTECTION CONSISTS OF

- a filtered internet service provided by HCC
- an up to date firewall provided by HCC
- up to date anti-virus software provided by HCC
- the Securus server which monitors and tracks all equipment and users connected to the network. This flags inappropriate usage against a pre-installed 'dictionary' taking a screenshot of the users screen and detailing the time, PC/laptop used, location of the hardware etc. As online safety is a child protection issue, monitoring the Securus server is undertaken by a Designated Safety Lead member of staff, currently either the Headteacher, Deputy Headteacher or Home-School Link

- all members of the Glenwood School community, including teaching practise students, Hampshire Futures staff, supply staff and any other visitor who will have access to the School's IT facilities sign an Acceptable Use Agreement (AUA). The AUA is discussed with pupils prior to them signing it. (There is a KS3 and KS4 version of the AUA)
- an encrypted wireless network (WPA 2 standard)
- ensuring staff have strong passwords i.e. an alphanumeric password, which is subject to six week change by server policy.

MONITORING OF INTERNET USE

- Glenwood School monitors usage of its Internet and email services without prior notification or authorisation from users.
- Users of Glenwood School's email and Internet services should have no expectation of privacy in anything they create, store, send or receive using Glenwood School's IT system.

POLICY PRINCIPLES

- Staff 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 Glenwood School and personal interests.
- Staff must not engage in activities involving social media, which might bring Glenwood School into disrepute.
- Staff must not represent their personal views as those of Glenwood School on any social media.
- Staff must not 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 at Glenwood School or give any details about their roles which identify Glenwood School as their place of work.
- 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 or Glenwood School.
- Staff must not use social media to express their discontent about their own role or any aspect about how Glenwood School operates. If there are any issues for staff in these areas, they must use the appropriate channels to raise them, in most instances this will initially be with their line manager.

PERSONAL USE OF SOCIAL MEDIA

- Staff members must not identify themselves as employees of Glenwood School 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
- Staff members must not have contact through any personal social media with any pupil, either present or former pupil; if unsure, please speak to the Headteacher.
- Staff members must not have any contact with a pupil's family members through personal social media, as that contact is likely to constitute a conflict of interest and may breach professional boundaries and relationships: if unsure, please speak to the Headteacher.
- If staff members wish to communicate with young people through social media sites, they can only do so with the approval of Glenwood School.
- Staff members must decline 'friend requests' from the pupils, either current or former, that they receive in their personal social media accounts. Instead, if they receive such requests who are not family members, they must inform the Headteacher.
- On leaving Glenwood School's employment, former staff members must not contact either current or former pupils by means of personal social media sites.

- Photographs, videos or any other types of image of pupils or staff identifying Glenwood School must not be published on staff's personal webspace.
- 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.
- 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 Glenwood School'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 if too much personal information is known in the work place.
- Staff members are strongly advised to set their privacy levels of their personal sites as strictly as they can and opt out of public listings on social networking sites to protect their own privacy.
- If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager. All communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended (social networking sites are public forums). You are strongly advised, in your own interests, to take steps to ensure as far as possible that their on-line personal data is not accessible to anybody who they do not want to have permission to access it.
- If you see social media content that disparages or reflects poorly on us, you should contact the Headteacher

BREACHES OF THE POLICY

Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Glenwood School's Disciplinary Policy and Procedure, which may result in dismissal.

Further information:

I. NASUWT, (2012). *Social networking – guidelines for members.* http://www.nasuwt.org.uk/InformationandAdvice/Professionalissues/SocialNetworking/NASUWT_007513

II. Safer Internet - http://www.saferinternet.org.uk

III. South West Grid for Learning Resources http://www.swgfl.org.uk/Staying-Safe

IV. For further information about the safe, secure and proper use of social media and networking sites, please see http://www.childnet.com/resources/social-networking-a-guide-for-teachers-and-professionals