

## SOCIAL MEDIA AND INTERNET POLICY

### General

The use of social networking sites on the internet has become an increasingly important part of life for many people. VTS recognises that this provides valuable opportunities for networking, marketing and an exchange of ideas. However, the widespread use of social networking sites and the possibilities of inappropriate use which may bring VTS into disrepute or compromise a member of staff and learners, means that a Policy is required. Whilst this is not definitive, social media services include Facebook, MySpace, Blogging, Twitter, YouTube, LinkedIn and includes the use of mobile telephones for text messaging.

Using the internet for research purposes is vital to learn and understand a variety of information. It is also integral to accessing advice and guidance. We actively promote our staff and learners to use the internet to gain knowledge, information, advice, and guidance. However, the internet can also contain harmful and inappropriate and misleading information that can compromise the safety and well-being of our staff and learners. This policy sets out how we ensure safe use of the internet.

### Social Media.

Social Media refers to a broad range of websites and services that allow people to connect with friends, family, and colleagues, online, as well as meet people with similar interests and hobbies.

The Policy applies to all staff in any role on a permanent, temporary, or fixed term basis and all learners. The policy also applies to the protection of our learners and our learners' expectations of use.

Access to social media sites using VTS computers is allowed in certain circumstances. However both staff and learners must ensure that access adheres to this policy, and does not interfere with work or academic duties.

VTS operates a Social Media site, Facebook, and makes comments on Twitter and Linked in. This is the responsibility of the Marketing Executive, and any posts made by or to any of these sites are moderated by the Marketing Assistant.

#### Responsibilities:

Staff should not accept offers from existing students to become a "friend" on their personal profile, as this could compromise VTS's Policy on Safeguarding and the Code of conduct.

Staff and learners should never post or send abusive, defamatory, or distasteful messages or post photographs, videos or other media which could be considered in breach of Policy and Procedure.

Staff must not post images or videos of staff or learners on VTS premises on their social media profile; however, staff are allowed to share pages from our own regulated social media platform.

Staff and learners will not publish personal identifiable information of VTS employees or students.

Staff and learners must not express opinions that profess to represent their own views on VTS.

Staff and learners must never post a comment about VTS that purports to represent the views of VTS, unless approved by the Managing Director.

Harassment or bullying via social media will not be tolerated. Ensure any comments made on sites could not constitute bullying, harassment, or discrimination.

Staff must also adhere to the principles contained within this Policy outside of working hours and may be subject to disciplinary action if they fail to do so. The inappropriate use of the Social Media sites may lead to disciplinary action.

Computers provided on site for learners to use block social media sites. These computers are for the use of internet research and completion of assignments and tasks, should learners wish to access their own social media platforms they must do so using their own devices.

We understand that our learners will use social media platforms outside of our onsite offices and for the majority of learners their research is conducted on their workplace or own personal computer, so we deliver a teaching session which teaches them about online safety and all learners must partake in this.

If your social media profile lists that VTS is your employer or that you are a learner at VTS, it should also state that any views expressed are your own and do not represent VTS.

Set your profiles to “private” to ensure control over who can access / view your information is restricted.

Be aware that Social Networking websites are a public forum, particularly if you are a part of a network. You should not assume that entries on any website will remain private and you are strongly advised to use the appropriate privacy settings.

Ensure conduct on sites could not be seen as detrimental to VTS or bring VTS into disrepute.

Take care not to allow interaction on websites that may cause to damage working relationships, for instance 'liking' a Facebook group with views that could be deemed extremist.

Be security conscious and take steps to protect yourself from identity theft, for example by restricting the amount of personal information given out. Social Media websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.

Change your social media password often.

Managers are responsible for ensuring that all staff or students for whom they are responsible are aware of this policy.

The Office Manager is responsible for the maintenance and monitoring of social media sites used onsite.

### **Internet.**

The internet is provided within in our offices and on tutor's laptops. Access to the internet in our Westcliff office is via 2 Wi-Fi passwords, one is VTS office, and one is as a VTS guest. Our Colchester office has a Wi-Fi password.

Tutors connect to the VTS office Wi-Fi whilst on site and their own Wi-Fi at home, all staff are provided with a 4G mobile network to add to their laptop to access internet within workplaces.

This policy also applies when accessing the internet in a workplace, café, home, or library.

Responsibilities:

The Internet should not be used to access or view illegal/offensive material including hate content, pornography, material that breaches copyright such as films or music, etc.

Transmission via email, forum, message board or other, of illegal content or content used to bully or 'troll' is prohibited.

Antivirus software must be up to date.

Reasonable personal use of the Internet is accepted for staff on their laptops or PC during their lunch break.

Internet use may be logged and monitored if any concerns of usage arise.

The DSL will monitor and ensure the computers used by learners to research and complete work have up to date anti-virus software and have filtering controls through a platform which is set by the DSL, so any harmful websites are blocked.

All learners must attend online safety training which includes internet safety.

The office manager and the administration team will monitor learner's internet search history after each usage.