**`1-\*+**

**.000.3**

**+2:?><Nnternet & Social Media Policy (Students).**

* + - visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
		- using the computer to perpetrate any form of fraud, or software, film or music piracy
		- using the internet to send offensive or harassing material to other users
		- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence
		- hacking into unauthorised areas
		- publishing defamatory and/or knowingly false material about Shockout, your colleagues and/or our customers on social networking sites, ‘blogs’ (online journals), ‘wikis and any online publishing format
		- undertaking deliberate activities that waste staff effort or networked resources
		- introducing any form of malicious software onto any Shockout laptops or desk top computer.
1. **Online Purchases**
	1. Anyone using PCs for a commercial transaction for example by entering their credit card details, does so at their own risk. Shockout Arts cannot be held responsible for losses resulting from sending confidential information via the internet.
2. **Copyright**
	1. Breaching copyright is illegal. It is the responsibility of the employee/student to keep within the law.
	2. Do not infringe any of the copyright regulations that apply to web pages. Unless specific permission is given on the website only a single copy may be downloaded and printed.
	3. You may download material and copy to a USB memory stick for the purposes of your private study, research, or for non-commercial purpose.
	4. In addition to the above you can also download and save into your One Drive or online in the Cloud on your One Drive.
3. **Business Hardware and Software**
	1. You must not damage Shockout computer hardware.
	2. Users are not allowed to delete, add or modify the software. We reserve the right to change PC software and settings without notice.
	3. Do not attempt to gain unauthorised access to any computer network or system.
	4. **Do not save work to the computer hard-drive** – it will be removed by cleaning software.
	5. Shockout shall have no liability for direct, indirect or consequential loss, however incurred, relating to data processed on, or any other use of the computer equipment.
	6. If a virus warning or other serious alerts are displayed on the computer, please tell a member of staff.
4. **Shockout Staff & Students**
	1. Teaching and Support Staff are responsible for ensuring that:
* They have an up-to-date awareness of e-safety matters and of the current college/university safeguarding policy, cyber security and procedures.
* They report any suspected misuse or problem to Management for investigation.
* Students understand and follow the safeguarding and cyber security of acceptable use in related policies.
* Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
* They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other college/university activities (where allowed)
* In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
	1. **Students are responsible for:**
* Using the college/university digital technology systems in accordance with Internet Policy.
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
* will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images.
* should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the college/university Internet Policy covers their actions out of college, if related to their membership of the university/college.

**8. Staff Social Media contact with Students**

8.1 Staff:

* Staff must not establish or seek to establish any contact with a student, via any channels including social media.
* All contact with students through personal contact channels is forbidden. All staff members should only use their Shockout email address to communicate with students and must not communicate with students on a personal email address, social media account or phone. All communication should be kept strictly to academic lessons, tutorials, one to one feedback sessions, SEND provisions, or safeguarding purposes using the formal correct channels of communication adhering to the communication policy.
* Shockout recognizes that staff members will encounter students outside of work. However, this should be limited, and we expect staff to use their professional judgment in any social situation and to report to their Designated Safeguarding Leads, if any contact with a student that they are concerned about or could be misinterpreted by students.
* Shockout students must not be encouraged to communicate with any personal social media accounts owned or managed by a staff member.
* Staff members are not allowed to accept friend requests from students, follow, like or share personal messages from a student.

**Student:**

* Students should not post videos of classes on Instagram, tik tok or any other forms of media without permission from their course coordinator or student co-ordinator.
* Any students that post or make any defamatory remarks regarding Shockout will face Disciplinary Procedure
* Be aware of cyber bullying and report to a member of staff.
* Any student found to be bullying a student will face Disciplinary Action (see Anti Bullying Policy and Disciplinary Policy)
* Shockout students must not communicate with any personal social media accounts owned or managed by a staff member.

**9. Disclaimers**

9.1 Shockout accepts no responsibility for technical malfunctions that may prevent access to the internet or web based e-mail services.

9.2 Shockout cannot accept responsibility for losses or problems caused by sending confidential information over the internet.

9.3 Shockout is bound under the Provisions of the Data Protection Act and will not release information on the use of specific internet resources by users except as required by law or as necessary for the proper operation IT breakout areas at the Velo Building.

**NB: Misuse of Shockout IT equipment can result in Disciplinary Action.**

**Related Policies**

Disciplinary

Anti Bullying