Online E-Safety and Social Media Policy			
Current Status	Operational	**Last Review:**	March 2024
Responsibility for Review:	Group Head of Pastoral Support and Administration	**Next Review:**	July 2025
Roles Responsible for Review:		**Originated:**	July 2021
Approved by:	SET Curriculum	**Committee:**	
Type of Policy:	(Staff / Students	**Quality Assured by:**	

1. Introduction

1.1. The Online E-Safety and Social Media Policy encompasses student use of the Internet, electronic communication and of mobile devices. It highlights the need to educate all students about the benefits and risks of using new technology and mobile devices and provides safeguards and awareness for users to enable them to control their online experiences. The College's Online E-Safety Policy operates in conjunction with other related policies and procedures.

1.2 Please note that this policy applies to both students and staff.

2. Context

2.1 Students and staff have access to the Internet, and email on all networked computers and computers/devices connected to the College Wi-Fi network in the College, for research and educational purposes. The Eastern Education Group welcomes this as a means for improving the IT skills of users, alongside the use of other new technologies, to better ensure equality for all its students regardless of protected characteristics or individual needs.

2.2 All students receive an induction when they enroll within eh Eastern Education Group, which includes online e-safety training.

2.3 Staff have mandatory online e-safety training once a year which is built into the annual safeguarding training.

2.4 The College online e-safety Policy complies with the following policies and legislation:

- Defamation Act 1996
- Criminal Justice and Public Order Act (1994)
- Equality Act 2010
- The General Data Protection Regulation
- The Copyright Designs and Patents Act (1988)
- The Computer Misuse Act (1990)

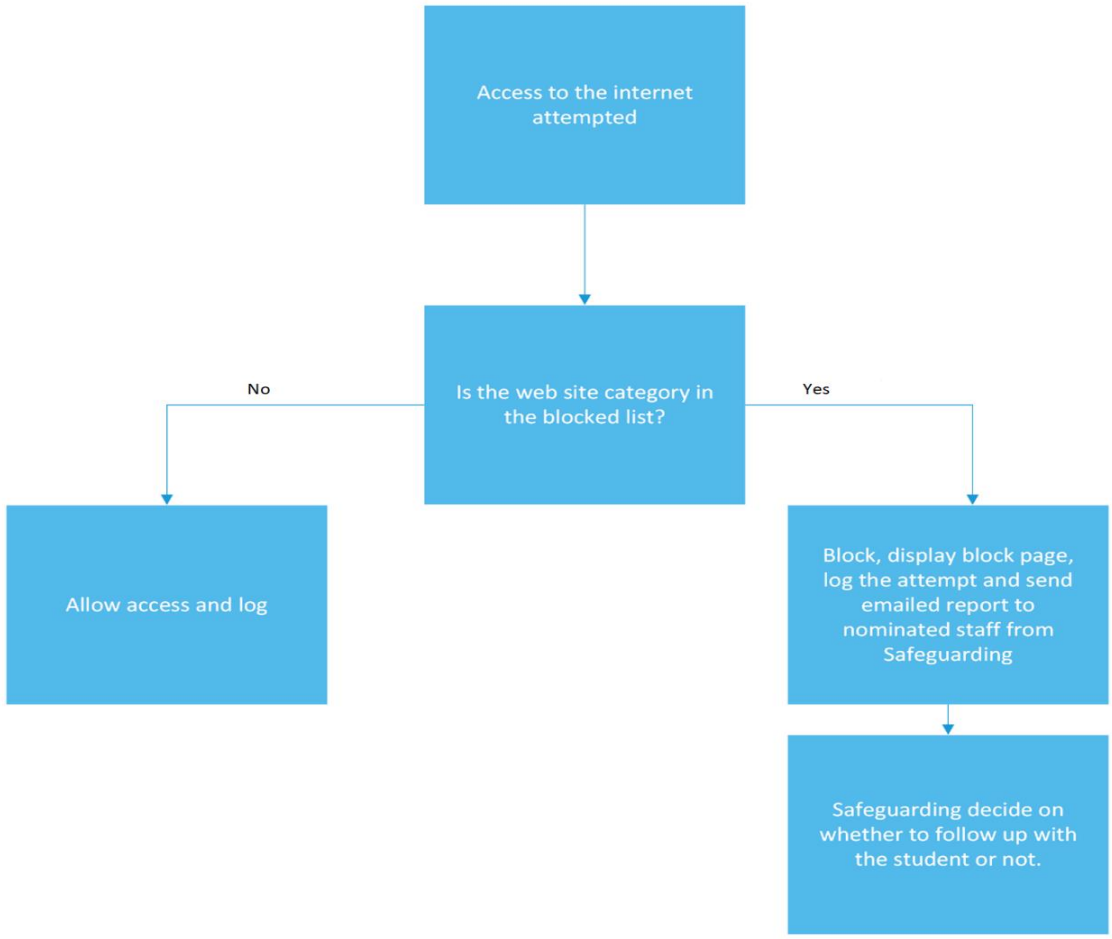
3. PROCEDURE

Internet Usage

3.1 Students and staff are encouraged to use the internet for educational research and students will be taught how to evaluate website content as part of their course.

3.2 Anyone accessing the College internet will do so via a unique password. An Internet filtering solution is in place to monitor and safeguard students and staff from accessing inappropriate sites; reports are reviewed and monitored to ensure that the filtering is appropriate and suitable for the age range of the students using the system. Where persistent offenders access inappropriate websites, the IT Services Manager may disable the student's user account, and the disciplinary process will be implemented as appropriate with the Head of Pastoral Support. The students' network access will be restored when the IT Services Manager has been notified that the issue has been resolved. Any staff accessing inappropriate sites will be subject to disciplinary action.

Web site filtering journey



3.3 Any person found to be deliberately re-routing access to avoid these restrictions will also be subject to College disciplinary proceedings.

3.4 The College Internet service is primarily for study–related purposes and any use of the system for private use should be outside scheduled class or study times. Users must accept full responsibility for personal bank data for example in using the College network when making private purchases online.

3.5 Be aware that the iBoss, Smoothball, Senso and Fortigate acceptable use policies strictly forbid the use of the service for any commercial activity.

3.6 The College takes reasonable steps to protect users from accidental exposure to explicit material. Any breaches of the policy must be reported to the nearest member of staff, a Personal Progress Tutor, the Senior Welfare Officer or the Head of Pastoral Support.

4. Internet Usage Rules

4.1 The rules detailed below apply whether the Internet is accessed via a College wired network connection or by one of the College's wireless networks.

4.2 Users must not attempt to access or upload on the Internet, information that is obscene, sexually explicit, racist and defamatory, incites or depicts violence, is extremist in nature or describes techniques for criminal or terrorist acts, in line with our Prevent Duty.

Blocked Categories	• Drug Abuse • Illegal or Unethical • Discrimination • Explicit violence • Extremist Groups • Child Abuse • Other Adult Materials • Gambling • Nudity and Risqué • Pornography

4.3 Users must not intentionally access or transmit computer viruses or attempt to 'hack' into data that may damage or breach the College network.

4.4 Users must not infringe copyright - this includes unauthorised copying of images from the Internet without permission and downloading of music files and commercial screensavers.

4.5 Users must not use the College Internet service for private commercial activity.

4.6 Users must not knowingly undertake any action that will bring the College or Education Group into disrepute.

4.7 Users must not attempt to deliberately re-route their connection to avoid the College proxy server or falsify usage logs in order to escape detection.

5. Social networking and personal publishing

5.1 Social Networks can be accessed via the College WIFI network available across the campus.

5.2 Users should be advised never to give out personal details of any kind which may identify them, or their location.

5.3 Users must not place personal photos, videos or music on any College network space unless approved by tutors in specific areas of the College for educational purposes.

5.4 Users should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Users should be encouraged to ensure that virtual communications areas are open only to known friends.

5.5 Staff must not use their own personal social media accounts for learning and communication, they must set up new accounts using the course name or vocational title. Staff must also not follow or friend this account with their own personal account. Staff are expected to moderate these sites with due care and diligence.

When posting on behalf of or as part of the Eastern Education Group or any of the establishments within this please ensure you adhere to these guidelines

1. **Seek Approval** – Messages that might act as a voice of the College must be approved by Senior Management

2. **Be Accurate** - Make sure that you have all the facts before you post. It's better to verify information with a source first than to have to post a correction or retraction later. Cite and link to your sources whenever possible - that's how you build a community.

3. **Be Transparent** - If you participate in or maintain a social media site on behalf of the Group or a College within the group, clearly state your role and goals. Keep in mind that if you are posting with a Group username, other users do not know you personally. They view what you post as coming from the Group. Be careful and be respectful. What you say directly reflects on the Group. Discuss with your manager the circumstances in which you are empowered to respond directly to users and when you may need approval.

4. **Be Responsible** - What you write is ultimately your responsibility. Participation in social computing on behalf of the Group or any college within the group is not a right but an opportunity, so please treat it seriously and with respect. If you want to participate on behalf of the Group, be sure to abide by its standard practice guidelines.

5. **Respect Others** - Users are free to discuss topics and disagree with one another, but please be respectful of others' opinions. You are more likely to achieve your goals if you are constructive and respectful while discussing a bad experience or disagreeing with a concept or person.

6. **Be a Valued Member** - If you join a social network like a Facebook group or comment on someone's blog, make sure you are contributing valuable insights. Post information about topics such as Group or individual college events or news only when you are sure

it will be of interest to readers. In some forums, self-promoting behaviour is viewed negatively and can lead to you being banned from websites or groups.

7. **Be Thoughtful** – If you have any questions about whether it is appropriate to write about certain kinds of material in your role ask your Tutor or manager before you post.

When posting as an Individual please ensure you adhere to the below guidelines

1. **Be Authentic** - Please be clear that you are sharing your personal views and are not speaking as a formal representative of Group or a College within the group. If you identify yourself as a member of the Group or a College within the group Community, ensure your profile and related content are consistent with how you wish to present yourself to colleagues.

2. **Use a Disclaimer -** If you publish content to any website outside of Group or a College within the group and it has something to do with the work you do or subjects associated with Group or a College within the group, use a disclaimer such as this: "The postings on this site are my own and do not represent Eastern Education Group or a College within the group's positions, strategies or opinions."

3. **Don't use the Group or a College within the group Logo or make Endorsements** - Do not use the Group or a College within the group marks or images on your personal online sites. Do not use Group or a College within the group name to promote or endorse any product, cause or political party or candidate.

4. **Protect your Identity** - While you should be honest about yourself, don't provide personal information that scam artists or identity thieves could use. Don't list your home address or telephone number. It is a good idea to create a separate e-mail address that is used only with social media sites.

5. **Does it pass the Publicity Test** - If the content of your message would not be acceptable for face-to-face conversation, over the telephone, or in another medium, it will not be acceptable for a social networking site. Ask yourself, would I want to see this published in the newspaper or posted on a billboard tomorrow or ten years from now?

6. **Respect your Audience -** Don't use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the Group or a College within the group's community. You should also show proper consideration for others' privacy and for topics that may be considered sensitive — such as politics and religion.

7. **Monitor Comments** - Most people who maintain social media sites welcome comments — it builds credibility and community. However, you may be able to set your site so that you can review and approve

comments before they appear. This allows you to respond in a timely way to comments. It also allows you to delete spam comments and to block any individuals who repeatedly post offensive or frivolous comments.

5.6 Staff must be mindful that they are in a position of trust and ensure that they do not post, like, tweet, re-tweet, share anything that could damage their own professional reputation or bring the college into disrepute by association, as their employer.

6. Email

6.1 The College uses a spam filtering system on the email. This monitors and blocks spam and other external email in order to protect College users and the system from offensive email, unnecessary email traffic and viruses sent by email.

6.2 All users will have access to email via their computer network account within the Group and are encouraged to use it as part of their learning. Students may also use private Internet services such as Google or Outlook Mail when using a Group computer.

6.3 However, email access opens up the Group to new risks and liabilities. Students must be aware that Group staff reserve the right to gain access to any email document sent by Students to recipients both inside and outside the Group and documents received onto the Group email from external bodies.

6.4 Student email boxes are set at defined limits by IT Services, which will not normally be extended except under special circumstances requested by a tutor.

7. Email Usage Rules

7.1 Downloading and passing on copyright information or material, which may be considered to be violent, obscene, abusive, racist or defamatory, will be treated by the Group as gross misconduct. Be aware that such material which may be contained in jokes sent by email can be considered to be harassment or bullying or in direct conflict to Prevent Duty. Any person receiving such email should report it to their tutor.

7.2 Users must not knowingly send or receive information that will bring the Group or a College within the group into disrepute.

7.3 Information sent by email will become subject to the rules under the General Data Protection Regulation, and this must be complied with.

7.4 Email must not be used for unsolicited advertising, and must not be used for the purposes of private commercial activity.

7.5 Persons sending emails must not flood the network by sending unnecessary information to all users. This uses bandwidth on the network, and server space, and may prevent important information getting through. This is particularly important when sending attachment files and documents.

Breach of these rules is a serious disciplinary offence and will result in the College taking action against the offender.

8. Handling E-safety Complaints

8.1 Complaints of Internet misuse will be dealt with by a Group Principal, The Group Head of Pastoral Care, The Group Head of Welfare and Safeguarding and HR

8.2 Complaints concerning safeguarding and child protection issues will be dealt with according to the Group Policy. Students, parents and staff will be informed of the complaints procedure.

Revision History – Online E-Safety and Social Media Policy

Revision date	Reason for revision	Section number	Changes made
Feb 2023	Annual review	throughout	references to OSFC changed to SAT
July 2023		1.5	Names of software systems updated
		Rubrik	Job title change/change of review date.
October 2023	EEG review	throughout	Reworded to cover EEG as 1 policy. Changes to formatting style throughout
		3.2	Web filtering diagram added
		Section 4	Blocked categories table added
			Appendices C & D removed