

Online E-Safety and Social Media Policy			
Current Status:	Operational	Last Review:	July 2025
Policy Owner:	Group Head of Pastoral Support and Administration	Next Review:	July 2026
Roles Responsible for Review:	SLT	Originated:	September 2019
Approved by:	SET Curriculum	Committee:	EEG Educational Excellence Committee
Type of Policy:	Staff / Students / External	Quality Assured by:	

1. Introduction

- 1.1. This policy applies to all students, staff and any other personnel associated with Eastern Education Group (EEG), which includes:
- Abbeygate Sixth Form College
 - Chalk Hill
 - Duke of Lancaster School
 - Exning Primary School
 - Stanton Primary School
 - One Sixth Form College
 - Priory School
 - Stone Lodge Academy
 - Sunrise Academy
 - West Suffolk College (including all PPL centres)
- 1.2 This policy encompasses student use of the internet, electronic communication and 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.

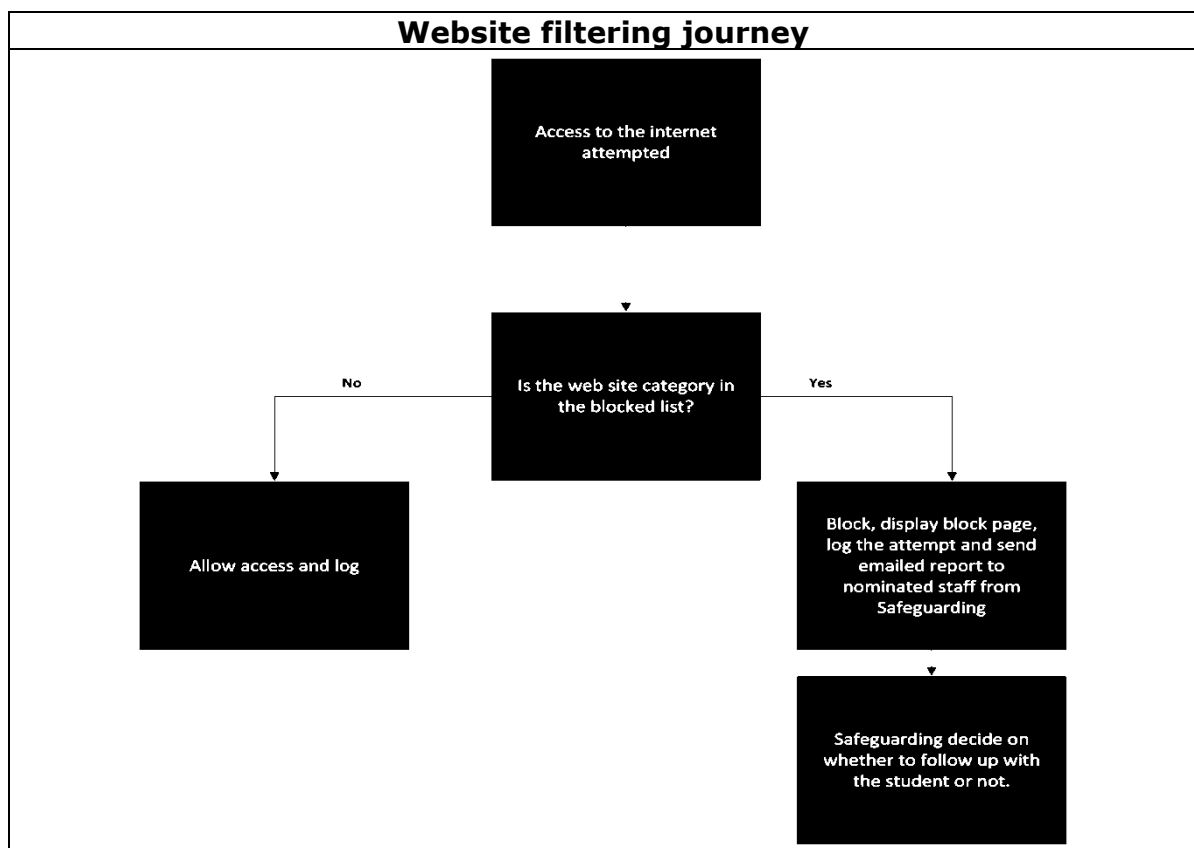
Context

- 2.1 Students and staff have access to the internet, and email on all networked computers and computers/devices connected to our Wi-Fi networks for research and educational purposes.
- 2.2 All students receive an induction and 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 This policy complies with the following 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 \(1990\)](#)

2. Procedure for 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 our internet will do so via a unique password and is subject to our internet filtering system which monitors and safeguards both students and staff from accessing inappropriate sites.
- 3.3 Reports from our internet filtering system are reviewed and monitored to ensure that the filtering is appropriate and suitable for the age range of the students using the system.
- 3.4 Where students or staff persistently attempt to access inappropriate websites, we may disable their account and implement our disciplinary process. Their access will be restored after the disciplinary process has been resolved.



- 3.5 Any person found to be deliberately re-routing access to avoid these restrictions will also be subject to our disciplinary proceedings.
- 3.6 Our internet service is primarily for study-related purposes and any use of the system for private use should be outside scheduled school/class or study times. Users must accept full responsibility for personal bank data, for example in using our network when making private purchases online.

3.7 Our internet filtering system:

- strictly forbids the use of the service for any commercial activity.
- screens content looking for key words and phrases, and logs and reports any inappropriate use of the internet.

3.7 EEG takes reasonable steps to protect users from accidental exposure to explicit material however any breaches of the policy must be reported to the nearest member of staff or the Head of Welfare and Safeguarding.

4. Internet Usage Rules

4.1 The rules detailed below apply to EEG internet accessed via wired and/or wireless networks.

4.2 Students and staff 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	<ul style="list-style-type: none">• Violence\racism• Intimate apparel\swimsuit• Nudism• Pornography• Weapons• Adult\mature content• Cult\occult• Drugs\illegal drugs• illegal skills\questionable skills• Sex education• Gambling• Hacking\proxy avoidance systems• Pay to surf sites• Internet Watch foundation CAIC blacklisted sites• Malware,• Radicalization/extremism
---------------------------	--

4.3 Students and staff must not intentionally access or transmit computer viruses or attempt to 'hack' into data that may damage or breach our network.

4.4 Students and staff must not infringe copyright - this includes unauthorized copying of images from the internet without permission and downloading of music files and commercial screensavers.

4.5 Students and staff must not use our internet service for private commercial activity.

4.6 Students and staff must not knowingly undertake any action that will bring EEG into disrepute.

- 4.7 Students and staff must not attempt to deliberately re-route their connection to avoid our 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 our Wi-Fi network.
- 5.2 Students and staff should be advised never to give out personal details of any kind which may identify them or their location.
- 5.3 Students and staff must not place personal photos, videos or music on any EEG network space unless approved by the SLT and for educational purposes.
- 5.4 Students should:
- be advised on security and encouraged to set passwords,
 - deny access to unknown individuals,
 - block unwanted communications
 - 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 work-related communications. Staff must set up new bespoke accounts for this purpose which clearly identify their job title. Staff may not follow/friend this new bespoke 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 EEG please ensure you adhere to these guidelines

- 1. Seek Approval** – Messages that might act as a voice of EEG must be approved by your SLT
- 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 EEG, clearly state your role and goals. Keep in mind that if you are posting with an EEG username, other users do not know you personally. They view what you post as coming from EEG. Be careful and be respectful. What you say directly reflects on EEG. 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 EEG is not a right but an opportunity, so please treat it seriously and with respect. If you want to participate on behalf of EEG 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 events or news only when you are sure it will be of interest to readers. In some forums, self-promoting behavior 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 adhere to these guidelines

- 1. Be Authentic** - Please be clear that you are sharing your personal views and are not speaking as a formal representative of EEG. If you identify yourself as a member of EEG 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 EEG and it has something to do with the work you do or subjects associated with EEG use a disclaimer such as this: "The postings on this site are my own and do not represent Eastern Education Group's positions, strategies or opinions."
- 3. Don't use EEG's logos or make endorsements** - Do not use EEG's marks or images on your personal online sites. Do not use EEG 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 EEG. 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.

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 EEG into disrepute by association, as their employer.

6. Email

- 1 EEG uses a spam filtering system on the email to monitor and block spam and other external email to protect students and staff and the system from offensive email, unnecessary email traffic and viruses sent by email.
- 2 All students have access to email via their EEG account and are encouraged to use it as part of their learning. However, students must be aware that EEG staff reserve the right to gain access to any email document sent by students and documents received from external bodies to their EEG account.

Email Usage Rules

- 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 EEG 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 or safeguarding lead.
- 2 Users must not knowingly send or receive information that will bring the Group or a College within the group into disrepute.
- 3 Information sent by email will become subject to the rules under the General Data Protection Regulation, and this must be complied with.
- 4 Email must not be used for unsolicited advertising and must not be used for the purposes of private commercial activity.
- 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.

7. Generative AI (GenAI)

- 7.1 Generative AI (GenAI) is now an integral part of the modern digital workspace, transforming how we learn, teach, work, and create. From summarising complex topics to drafting communications, GenAI tools enhance productivity, foster creativity, and support inclusive learning.
- 7.2 An AI Executive Board has been set up to provide guidance and support to staff and students when using GenAI. Refer to The Acceptable Use of Generative AI (GenAI) policy for more information.

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

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

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 complaint's 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			Reworded to cover EEG as 1 policy.
Jul 2024	Annual review	1.1	Updated to include SENDAT and Exning.
Jul 2025	Annual review	7.1-7.2	Addition of a section on GenAI p.7