Online E-Safety and Social Media Policy

Online E-Safety and Social Media Policy Appendix B – ICT User Agreement – students			
Current Status	Operational	**Last Review:**	July 2024
Responsibility for Review:	Group Head of Pastoral Support and Administration	**Next Review:**	August 2025
Internal Approval:	SET Curriculum	**Originated:**	September 2019

All users requiring access to the college network or Internet must agree to the proper use of Eastern Education Group ICT resources and sign a copy of this statement. Users who fail to follow this agreement may be denied access to some, or all, of the college's resources and disciplinary procedures may be invoked.

The computer system is owned by the college and is made available to students to further their education and to staff to enhance their professional activities during teaching, research, administration, and management.

The college reserves the right to examine or delete any files that may be held on its ICT system, to monitor any internet sites visited or examine any e-mails.

I understand and accept that:

1. This Agreement covers the Groups ICT system even when access is made to the system from a personal device used on the BYOD programme, home computer or other similar device via the Internet.
2. Access to the resource can be made only via the User's own username and password.
3. Users must not make their Username or Password available to any other person and must lock their session before leaving the computer unattended. If a user suspects that their password has been compromised, they should change it immediately and seek advice from the IT Service Desk.
4. All activities utilising the Groups systems should be appropriate to the enhancement of the student's education.
5. The Group actively discourages all students from using USB flash drives to store work. Students must ensure that they have multiple copies of coursework, or it is saved on OneDrive which can then be accessed from any Internet enabled device. Further advice can be sought from the IT Service Desk.
6. Copyright of materials must be respected, including but not limited to; music, film, games, resources, and data.
7. Use of the network to access inappropriate materials (e.g. 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 black listed sites, Malware, radicalisation\extremism is forbidden.
8. Unauthorised use for personal financial gain, gambling, political purposes, or advertising is forbidden.

9. Activity that threatens the integrity of the groups' ICT systems, or activity that attacks or corrupts ICT systems is forbidden, including attaching unauthorised electronic media or devices.

10. Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received. Posting anonymous messages and/or forwarding chain mail is forbidden.

11. Language and content used for any electronic communication should be as is acceptable for normal work.

12. The inappropriate use of social network sites, which brings the Group into disrepute or causes offence to students or staff is not acceptable. Eastern Education Group expects students to use social networking sites such as Instagram, YouTube, and Twitter in a mature and responsible manner.

13. When submitting an assignment, it is my responsibility to print my own work. To support this the college will provide me with a termly printing allowance which I will have the ability to top up.

14. Any technology designed to avoid or bypass the education setting or other establishment filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.

15. All internet use is logged on any device utilising the college's Internet connection.

16. All faults and damage must be reported to the IT Service Desk or your teacher.

17. Caution must be exercised when opening email attachments or clicking links in emails, even when the sender is recognised.

18. To join the BYOD wireless network, you will be required to install a security certificate on your device.

19. The use of personal hotspots is forbidden. The college may use technical methods to disable their use.

20. The date/time/computer name is recorded upon logon and will be used in the event of investigating any damage to equipment.

21. All vandalism to college equipment will be investigated and students may be charged where the Group believes there is reasonable evidence to suggest the damage was willful.

I will:

1. Notify a member of staff if I receive unpleasant messages or other material

2. Respect the college's ICT equipment and use it suitably and with care