SWANSEA COLLEGE
Building foundations for your future

Student Guidelines for Internet use

Student guidelines for Internet use

Students' Classroom (access details will be given by the tutor during the induction process) and this includes timetables, handbook, all student policies, Leave of Authorisation Form (online) and Absence Form (online).

Internet usage:

- Students are responsible for good behaviour on the Internet just as they are in a classroom or a college corridor. General college rules apply. The Internet at the college is provided for students to conduct research and access their online classroom and work. Remember that access is a privilege, not a right, and that access requires responsibility.
- Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with college standards and will honour the agreements they have signed. Staff may review student files and communications to ensure that they are using the system responsibly. Users should not expect that files stored on the servers are private. The admin staff will, as a matter of course, review user directories and delete any unnecessary material that is considered to be taking up unacceptable amounts of disc space.
- During college hours, teachers will guide students toward appropriate materials. Outside of college, families are responsible for such guidance as students must also familiarise themselves with other information sources such as television, telephones, movies, radio and other potentially offensive media.

Unacceptable use of the network may include:

Illegal activities

- Sending or displaying offensive messages or pictures, to include "sexting" (the distribution of sexually explicit material)
- Accessing, uploading, downloading or distributing pornographic material on college computers or personal computers used in college
- Violating copyright laws
- Accessing or downloading any material in violation of the law
- Cracking (unauthorised attempt to discover a computer password)
- Hacking (unauthorised attempt to bypass security)
- Impersonation (the act of pretending to be someone else by setting up a false profile, or stealing someone's password to post false material that will endanger them, cause them distress or cause them to be falsely accused)

Inappropriate language & harassment in electronic communication

- Using vulgar or obscene language in any electronic communication
- Harassing, insulting, defaming, denigrating, or attacking others
- Spamming other users by sending unsolicited junk emails (including chain letters)
- Commenting on 'blogs' or without permission of the supervising teacher
- Cyber stalking (cyber threats or blackmail using digital resources)
- Outing (deliberately sharing someone's personal or sensitive information)

Endangering personal safety

- Revealing personal contact information (home address, telephone number, personal details, ID numbers, etc.) to other individuals over the Internet.
- Arranging to meet people contacted over the internet without approval

Breaching system security

- Intentionally spreading viruses, worms, chain letters, or Trojans
- Vandalising computers or peripheral equipment, computer systems or computer networks
- Altering, moving or deleting the files belonging to others
- Using another person's password, or providing your password to another person
- Unauthorised attempt to access the network, including use of the network on someone else's login
- Attempting to access the network without providing the assigned user name and password at the log-on screen
- Using any internet 'service' that attempts to "spoof", "mask" or 'hide' its identity from college network security e.g. 'proxy' sites or proxy anonymisers

Invading privacy

- Trespassing in someone else's folders, work or files
- Reposting a message that was sent to you privately, without permission of the original sender

Misuse of limited resources

- Use of the network for commercial purposes

Misuse of technologies

- Accessing instant messaging or social networking websites during college hours on personal devices
- Accessing instant messaging or social networking websites on the college laptop or computer
- Signing into any web-based service, requiring personal details in exchange for a username

and password for further access not explicitly authorised by the teacher
- Posting unauthorised college information via video or audio to public spaces, e.g. YouTube, Instagram, Tiktok and all other social networking apps, either as a member or anonymously
- Altering, deleting or moving any digital materials produced on any 'social space 'without the permission of the owner
- Commenting on other people's work appearing in any space within the public domain without the permission of the teacher
- Publishing any copyrighted materials provided to students in the class to the public domain (as a teacher and college-generated media are subject to copyright)
- Posting, downloading or plagiarising any work posted to social spaces as reference materials
- Digital information supplied by staff to students in the course of their studies must not be published in any form to the public domain. Materials are subject to copyright and remain the property of the college at all times
- Accessing games and personal entertainment sites not directly related to the area of study at the time of access

Extremism

Accessing of extremist websites or other media is not allowed. Any breach of this will be reported to the Principal and students may find be subject to disciplinary procedures *including referral to the Channel prevention programme.*

Infractions of the acceptable use policy will be dealt with according to the college discipline policy.