WSFC Acceptable Use Policy For Students & Visitors

Introduction to the Acceptable Use Policy

It is essential that the IT resources and facilities provided by College are used in a responsible manner, thus ensuring that as many users as possible can take advantage of this valuable resource in a safe and productive manner.

All users (staff, students and visitors) of the computing facilities of the College are automatically bound by the terms of this Acceptable Use Policy (AUP) - by using the College's computing facilities you show your acceptance of this AUP.

This policy may be revised from time to time, and you are bound by the terms of the latest version. Any changes to the AUP will be notified via the message boards on the College gateway.

This policy should be read in conjunction with the Student Code of Conduct Policy, and the Anti-bullying and Anti-Cyber bullying Policies, which are available via the Gateway.

Internet Service Provider's AUP

Internet access in the College is provided by janet, and access to the internet is governed by the terms of their AUP. Any part of the WSFC policy that relates to internet use is in addition to our provider's AUP.

janet AUP

Use of Athens is governed by the terms of their policy, available at HTTPS://openathens.org/terms-conditions-openathens

General use

You must not:

- connect a device to the College Wi-Fi that does not have up to date antivirus software installed or the latest security patches, or be a jailbroken Apple device from Apple for your iPad or iPhone or be a Jailbroken device
- create, store, transmit or knowingly receive any extremist material. (Extremism is defined as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance for those with different faiths and beliefs. It includes calls for the death of members of the British armed forces, whether in this country or overseas.)
- create, store, transmit or knowingly receive any fraudulent, offensive, defamatory, obscene, indecent or hurtful images, data or other material, or any data capable of being resolved into such material
- create, store, transmit or knowingly receive any material that is detrimental to the College's reputation, or that of its staff or students

- make personal comments about staff or students on internet forums, via email or internet sites including social networking sites
- use material in such a manner that applicable copyright laws are violated
- use open access facilities for non-College work use, for example you must not use the LRC computers for playing games or streaming non-educational content
- allow others to use their network account, or use someone else's network account with or without their permission
- install software on any of the College computers unless specifically authorised to do so
- join a device to the College domain
- attach any device to the College network e.g. by using a network cable other than via the College Wifi network
- cause physical damage to College resources
- be in possession of software that could be used to violate the privacy of other users (such software includes, but is not limited to, port scanners, password crackers, remote machine monitors and network traffic sniffers)
- undertake activities which:
    - use the facilities in any way that denies service or causes inconvenience to other users
    - attempt to bypass any security, anti-virus, monitoring or blocking features
    - make unreasonable demands of network resources

Private use of College computing facilities

Private use of College computing facilities in your free time is acceptable, subject to the terms below.

- Students must refrain from private use if requested to do so by any member of staff
- Private use by students during lessons is prohibited unless permission is obtained from the member of staff running that lesson

Private use must not:

- Make unreasonable demands of network resources, including internet bandwidth
- Interfere with your ability to carry out the tasks expected of you
- Prevent others from carrying out College related work
- Break the terms of this AUP

While you are free to use the College's facilities to access password protected services such as eBay, Amazon, Hotmail etc., you do so entirely at your own risk. The College accepts no responsibility for the security and integrity of data transmitted or received as part of a password protected session as it passes through our systems.

Accessing from home

All accesses to the College's IT facilities from outside the College are still bound by the terms of this AUP.

All reasonable effort must be made to ensure that College materials are not accessible to persons not connected with the College.

While every effort is made to ensure the integrity of available materials, the College offers no guarantee that files are free of viruses, and users should ensure that any downloaded item is checked on their local machine before use.

Monitoring the use of IT resources and facilities, and inappropriate Internet content

The College reserves the right to monitor the use of IT resources and facilities by staff, students and visitors to ensure that College Policies, including the AUP, are not broken and devices connected to the College WiFi network are not infected with viruses or malware.

Those responsible for monitoring the College network will at all times show discretion and respect the privacy of an individual if private or personal information is revealed as a result of random monitoring, as long as such information does not break the terms of this AUP and is not considered to be in violation of applicable UK law.

The College screens websites and filters internet access to inappropriate content, including extremist material. The College will record any attempt to access the following inappropriate content and this may lead to disciplinary action, the outcome of which is likely to be suspension or exclusion.

- Violence/hate/racism
- Intimate apparel/swimsuit
- Nudism
- Pornography
- Weapons
- Adult/Mature content
- Cult/Occult
- Drugs/Illegal Drugs
- Illegal skills/Questionable skills
- Sex Education
- Gambling
- Alcohol/Tobacco
- Games
- Hacking/Proxy avoidance systems
- Personals and dating

Any offence under English Criminal Law will be referred to the relevant police (or other) authorities.

What will happen if you break the AUP

Breaking the Acceptable Use Policy will lead to disciplinary action which may result in suspension or exclusion. Please note that this will extend to activities unrelated to College where these bring the College into disrepute or suggest that staff, students, visitors or other members of the College would not be safe should the person concerned continue to be a member of the College.

A major violation of the AUP, such as extremism, accessing pornography or trying to break the network, will result in disciplinary action which may result in exclusion or suspension.

Minor violations of the AUP will result in disciplinary action which may initially result in warnings, fines, the temporary loss of access to the IT network, and if repeated exclusion or suspension.

Any offence under English Criminal Law will be referred to the relevant police (or other) authorities.

Blocking of devices suspected to contain virus or malware

The College reserves the right to block any device from using the College Wifi network that is suspected of being infected with a virus or malware, or of using software with malicious or illegal intent.

This block will stay in place indefinitely unless the user can demonstrate following criteria is met:

- up to date antivirus is installed where applicable
- the latest security patches from all accepted software providers
- Jailbroken devices would require a stock iOS to be installed

If subsequently the device is suspected again, it is at the Colleges discretion if the block is lifted or will stay in place indefinitely.

EYS February 2018