Worcester Sixth Form College

Acceptable Use Policy For Staff

Introduction

This Policy incorporates, and updates, the previously separate Acceptable Use Policy, Monitoring Employee Communications Policy and Social Networking 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 employees using 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, in which case you will be notified via the message boards on the College gateway.

Employers have a right to monitor the communications of their employees whilst they are at work. In fact they have a duty to do so where they believe, or are aware, that such communications might be illegal or the cause of unwanted harassment or bullying. On the other hand employees have a right to privacy that would include personal communications to or from their place of work. It is clear that it is not reasonable for an employer to assume that an employee never makes private calls or sends personal messages. However between the extremes of illegal activity and the occasional urgent or emergency personal message there is a range of behaviour within which each party should behave reasonably.

This policy explains what is regarded as a reasonable level of personal employee communications and sets out the College's policy on monitoring this. There is an obvious distinction between monitoring the level of personal communications and monitoring the content of them.

This Policy aims to outline the responsibilities of employees when accessing social media either personally or using it for College purposes. It aims to manage organisational risks when social media is used for both business and personal use, and to ensure that its use is acceptable to avoid bringing the College into disrepute. The College's preferred Virtual Learning Environment is hosted on Moodle, however we recognise that some staff choose to encourage students to use other Virtual Learning Environments on social media, forums or networks such as Facebook or Twitter. It is important that all interactions between staff and students are conducted in a safe and professional manner.

Breaking the terms of the AUP This policy should be read in conjunction with the staff Code of Conduct.

A, 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 device
- create, store, transmit or knowingly receive any extremist material (see appendix 1)
- 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 College IT facilities, including the internet, in ways that cause distress and anxiety to colleagues or other members of the College;
- use College IT facilities, including the internet, for personal use during teaching contact time (other than very briefly in exceptional circumstances)
- use material in such a manner that applicable copyright laws are violated
- 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
- attach any device to the College network e.g. by using a network cable other than via the College Wifi network
- join a device to the College domain
- 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, including data storage and internet bandwidth

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

Accessing from home

All access to the College's facilities from outside is 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.

Staff **must not** use a public WiFi connection to access College resources unless it is via a trusted VPN provider e.g. Avast VPN.

Staff responsibility in relation to Extremism

Staff must take responsibility for, and be committed to, promoting and safeguarding the welfare of children, young persons and vulnerable adults whether responsible for, or in contact with, them. Staff must not ignore, initiate or encourage extremism. This includes the requirement to be alert to the risks of how students can be drawn into extremism and to pass any suspicions or relevant information to the Single Point of Contact, the Designated Safeguarding Lead, or, in her absence, any member of the College's Safeguarding Team.

If a member of staff considers it is appropriate for students to access or interact with potentially sensitive or extremist material as part of their studies, it is the responsibility of that member of staff to:

1. seek the agreement of their Head of Department
2. conduct a risk assessment which identifies the potential risks and appropriate controls to promote student safety
3. submits the risk assessment to and receives authorisation by the Deputy Principal for the activity or task in question

Personal use of College IT resources and facilities

Although the College IT resources and facilities, including email and internet, are primarily for business use the College understands that employees may on occasion need to use the internet for personal use. Employees may access the internet at work for personal purposes provided that:

- such use is limited to no more than 20 minutes in any day during working time;

- College IT resources and facilities, including the internet, are not used for personal use during teaching contact time other than very briefly in exceptional circumstances
- such use is consistent with the rules and procedures in the AUP
- employees do not enter into any contracts or commitments in the name of or on behalf of the College, unless authorised to do so;

Reasonable personal use of computing and telecoms systems by staff might include the following:

- Making, or altering, appointments with doctors, dentists, etc.
- Communication with a child minder or carer where this is necessary in relation to the welfare of a child or relative or the arrangements made with the child minder or carer.
- Communication with relatives in the event of family illness, accident or other emergency.
- Contacting a child's school in the event of a problem.
- Altering personal or social arrangements in the event of being asked to work late.
- Limited personal banking transactions.
- Job related training or education.
- Telephone calls in relation to matters relating to work being done to the employee's property.

This is not meant to be a definitive or exhaustive list and staff should use their discretion about urgent or emergency use that is reasonable. Guidance will be provided by senior staff or the Personnel section if needed.

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

The College reserves the right to monitor employees' internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it.

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 considers the following to be valid reasons for checking an employee's internet usage:

- If the College suspects that the employee has a device connected to the College WiFi network that is infected with a virus or victim of malware
- If the College suspects that the employee has been viewing offensive or illegal material, such as material containing racist terminology or nudity (although the

College understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case).
- If the College suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.
- If the College suspects that the employee has broken the terms of the AUP or other College Policy

The College reserves the right to retain information that it has gathered on employees' use of the internet for a period of one year.

In those extreme cases where it is thought an employee is guilty of harassment or bullying or undertaking or planning illegal activity, the content of communications would be monitored. In these cases it is likely the employee would not be informed and if necessary the police would be involved. Following the investigation disciplinary or other action would be taken if appropriate.

In extreme circumstances intervention may include a search of an employee's desk or workstation area.

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.

- 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

It is possible to allow access to blocked sites for legitimate research. If a member of staff or their students needed to research blocked sites they should discuss this with their Head of Department in the first instance and seek approval from the Deputy Principal.

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 employee 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.

B, MONITORING EMPLOYEE COMMUNICATIONS

Principles

- All monitoring of employee communications must be in pursuit of a legitimate aim and carried out in accordance with legislation governing the monitoring of employees communications (see Appendix 2).
- Any intervention must be necessary and proportionate to the concern identified.
- Except in lawful circumstances any employee would automatically be informed if their communications were being monitored and the dates during which this would occur. The Regulation of Investigatory Powers Act is not applicable unless an employee's consent is obtained.
- The College expects the duty of trust of its employees to be fulfilled by their commitment to the aims and purposes of the College and not to unreasonably use their employed time to pursue personal aims and interests.
- 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.

Definition of Employee Communications

Employee (including self-employed contractors, agency workers, volunteers or any other individuals working temporarily in the College) communications could include any or all of the following:

- Emails, both inward and outward, internal and external.
- Telephone calls, both internal and external, made and received.
- Internet usage – sites, range of frequency and duration.
- Incoming and outgoing mail.
- Records or logs of any of the above where these are available.
- Any other form of communication that might be a legitimate source of investigation.

Reasons for Intervention

The College reserves the right to undertake routine monitoring of phone calls or other communications, e.g. dates, telephone numbers, duration, etc. to analyse telephone bills or Internet usage. This would be action under RIPA and would not consist of personal data unless a member of staff was notified beforehand that they could be identified through the process.

If misuse was suspected it would fall broadly within the following categories:

- Misuse of facilities or equipment perhaps preventing its legitimate use by others or preventing the employee from carrying out their duties effectively.
- An unreasonable amount of time, more than several minutes a day of employed time, was being used in personal communication.
- The employee was imposing unreasonable costs on the College for private benefit.

Where these concerns arise an employee will be informed that their communications are being monitored and necessary action taken where this is regarded as being excessive.

Monitoring of email

The College reserves the right to monitor employees' emails, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The College considers the following to be valid reasons for checking an employee's email:

- If the employee is absent for any reason and communications must be checked for the smooth running of the College to continue.
- If the College suspects that the employee has been viewing or sending offensive, extremist or illegal material, such as material containing racist terminology, extremist content or nudity (although the College understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the College suspects that an employee has been using the email system to send and receive an excessive number of personal communications.
- If the College suspects that the employee is sending or receiving emails that are detrimental to the College.

When monitoring emails, the College will, save in exceptional circumstances, confine itself to looking at the address and heading of the emails. Employees should mark any personal emails as such and encourage those who send them to do the same. The College will avoid, where possible, opening emails clearly marked as private or personal.

The College reserves the right to retain information that it has gathered on employees' use of email for a period of one year.

Staff should be aware that some of their emails might also be viewed as part of monitoring being undertaken of communications by a student or another member of staff.

C, USE OF SOCIAL MEDIA

Staff must not:

- Invite existing students at the College to become their 'friends' on Facebook **(or similar on other social network sites)**.
- Accept invitations from existing students at the College to become 'friends' on Facebook **(or similar on other social network sites)**.
- Post any negative or inaccurate information about the College on Social Media.
- Post anything on Social Media which would reflect poorly on the College or bring the College into disrepute.
- Post any photographs or video clips of activities that take place at College or related to College activities without checking with the member of the SMT responsible for marketing (who will know whether there is permission from students for this information to be used).
- Post contact details for any member of staff or student at the College on Social Media (or any other information that might result in a breach of the Data Protection Act).
- Set up any other groups or pages relating to the College without agreement from your Head of Department or line manager, in addition to submitting a risk assessment and obtaining permission from the Deputy Principal.
- Use social media during normal working hours to socialise with friends when they should be working.

If staff become 'friends' with past students or work colleagues on Facebook (or similar on other Social Media), they should adhere to the code of conduct with regard to not bringing the College into disrepute.

Employees are advised to refrain from publishing any personal or sensitive information on Social Media.

Inappropriate or offensive material on social media

Any concerns regarding the safety of learners, including extremist activity, must be referred to the Designated Safeguarding Lead and the Prevent Single Point of Contact.

If staff are aware of inappropriate or offensive material on social media that relates to the College they must report it to the Designated Safeguarding Lead and the member of the SMT responsible for marketing. If it relates to a current student there are disciplinary procedures that can be followed and the item in question may be removed.

Staff must not post replies to negative comments or discussions that students have made about the College or individual members of staff on social media (whether it be

the official College Facebook page or other unofficial pages) as to do so encourages an online argument which can get out of hand. Instead, staff must bring this matter to the attention of their Head of Department or line manager and to the member of SMT responsible for marketing.

Students accessing inappropriate or offensive material as part of their course

If a member of staff considers it is appropriate for students to access or interact with potentially sensitive or extremist material as part of their course, it is the responsibility of that member of staff to:

- seek the agreement of their Head of Department
- conduct a risk assessment which identifies the potential risks and appropriate controls to promote student safety
- submit the risk assessment to and receive authorisation by the Deputy Principal for the activity or task in question

Privacy settings and personal information

Default privacy settings on social media may allow for some information to be shared beyond an individual's contacts. In such situations the user is personally responsible for adjusting the privacy setting for the account. Information available on social media may be used as evidence as part of College disciplinary procedures or legal proceedings.

When engaged in College related activity staff must review their access and privacy settings on social media to control who can access their personal information. If staff permit students to use social media for College related activity it is their responsibility to ensure that students review their access and privacy settings on social media to control who can access their personal information, and to ensure that students do not publish any sensitive or personal information.

Monitoring & Review
This policy will be monitored by the Deputy Principal and the Personnel Manager and reviewed annually by the Senior Management Team. Where significant alterations are intended they will be reported to the Governing Body Resources Committee.

EYS February 2018

Appendix 1 Definitions

Extremism

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.

Employee

The term employee is used interchangeably with staff in this policy and includes self-employed contractors, agency workers, volunteers or any other individuals working temporarily in the College)

Social Media

Social Media is the term used to describe online tools, websites and interactive media that enable users to interact with each other in various ways, through sharing information, opinions, knowledge and interests. Social Media involves building online communities or networks which encourage participation, dialogue and involvement.

Reference to Facebook throughout this Policy should be taken to refer to other similar social networking sites where appropriate.

Appendix 2 Legislation governing the monitoring of employees communications

Legal Context

The legal context in which communications can or cannot be monitored is covered by several pieces of legislation:

(i) Article 8 of the European Convention on Human Rights states that:

- "Everyone has the right to respect for his private and family life, his home and his correspondence" (Article 8 (1)).
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (Article 8 (2)).

(ii) Legislation governing the rights of employers to monitor employees' communications includes:

- The Data Protection Act 1998 – the Employment Practices Data Protection Code Part 3: Monitoring at work, which covers monitoring of staff at work,
- The Regulation of Investigatory Powers Act 2000 (RIPA) – which concerns the 'interception of a communication in the course of transmission' and, as regulatory support for this legislation,
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 – which provide that in certain circumstances in business it is lawful to intercept communications without consent. The Regulations state that if the College:
  - intends to make interceptions without consent for the purposes authorised under the regulations, it must make all reasonable efforts to inform every person who may use their telecoms system that communications may be intercepted. This may be done through a contractual clause or other readily available literature.
  - wishes to make interceptions outside the scope of the regulations it will need to gain the consent of the sender and the intended recipient of the communication. Interception would be authorised where the College believed it had reasonable grounds to believe that it had the consent of both the sender and the intended recipient of the communication, eg. through a contractual clause or message at the beginning of each call to say it was being recorded or monitored.