ACCEPTABLE USE POLICY (STUDENT) 2025/26

Aim

It is important that all users take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

All users have a responsibility to use the college's computer systems in an appropriate, lawful, and ethical manner.

To ensure that students are fully aware of their responsibilities when using technology, they are asked to read this Acceptable Use Policy.

Scope

This policy applies to all students within the college community who have access to the college IT systems, both on the premises and remotely. This policy applies to all use of technology including use of college and personal devices.

This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK). Keeping children safe in education guidance means the College has a statutory duty to carry out appropriate filtering and monitoring. The College also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

All potential IT systems users are required to adhere to the AUP policy and regulations and the Online Safety Policy and Procedures upon joining the college.

Acceptable Use Policy Statements and Terms

This is not an exhaustive list and all students are reminded that IT use should be consistent with the college ethos, college policies and the Law.

Accepting Worcester Sixth Form Colleges AUP means you abide by the following principles:

1. Safety, filtering and monitoring

- I will only use college systems on devices with current security updates.
- The college's **internet filter** is intended for user protection and should not be bypassed, nor specific access or passwords be shared.
- I will ensure my internet use is safe, legal, and understand offline consequences of online actions.
- I know my activity on college devices and networks is **monitored** to protect me and enforce the Acceptable Use Policy (AUP).
- I am aware that not everyone online is genuine and will seek advice if I'm unsure about someone's identity or intentions.

2. **Passwords and Privacy**
    - I will keep my passwords confidential and regularly verify that my privacy settings are appropriately secured.
    - I will carefully consider before sharing any personal information.
    - I understand the importance of safeguarding my password to protect my privacy, academic work, and personal safety.
    - I will utilise multi-factor authentication (MFA) when required.
    - Accessing or modifying other people's accounts or information is not permitted.
    - I will not store personal information (e.g., personal photographs, files, emails, or financial information) on college network or devices.
    - I acknowledge that any stored private data may be discoverable in searches and accessible by authorised staff in incident investigations or subject access requests and could potentially be disclosed to third parties as required.

3. **Responsible**
    - Personal devices or mobile phones **may only** be used in lessons with **permission**.
    - Consuming food or drink is not allowed in IT rooms.
    - College computers, devices, and internet access are intended for learning and work-related purposes; other uses may be restricted.
    - All electronic communications should be composed carefully and politely, with awareness that messages might viewed by unintended recipients.
    - Changes to computer settings should only be with technician approval.
    - Use of the college's IT system for personal financial gain, gambling, unlawful activity, political activities, or advertising is not permitted.
    - In cases of suspected inappropriate use of technology, the college may implement enhanced monitoring, including review or confiscation of loaned personal devices.
    - Users are responsible for devices or equipment loaned to them and must cover repair or replacement costs if items are stolen or damaged beyond standard wear and tear during the loan period.

4. **Work Authenticity and Plagiarism**
    - I will check the reliability of information I get from online sources.
    - I will respect others' information and copyright by giving references when using images or text in my work.
    - Work submitted for formal assessment must be the student's own, original work, not copied or paraphrased from external sources, including any **AI tools or humanisers**, and must reflect independent effort.

- Use of AI that prevents students from independently demonstrating achievement may be considered malpractice. AI tools may only be used for assessment if specifically permitted, and all submissions must represent the student's independent work and thought.
- I am aware the college employs various methods to **verify the authenticity** of submitted work to comply with exam board rules.
- Investigations into malpractice may lead to incidents being reported to relevant authorities or external agencies resulting in disqualification from examinations.

5. **Bullying, harassment and permission**
   - I will not use technology to be unkind to others. Bullying, both online and offline, is not tolerated, whether inside or outside college hours.
   - Technology must not be used for harassment or to upload content that could upset, threaten, or offend anyone in the college community.
   - Uploading images or videos of others online should only occur when content is appropriate and permission has been granted.
   - I will think before posting, knowing that once something is uploaded, it can become public, difficult to delete and potentially be illegal.
   - Harassment and discrimination are unlawful, regardless of whether College IT systems are involved.

6. **Legal**
   - Attempting to/or hacking accounts or systems is against college policy and may be a criminal office.
   - Sending threatening and offensive messages, downloading or sharing inappropriate material online is against college policy and can be a criminal offence.
   - IT usage is **monitored** for safeguarding reasons and to identify signs of extremism, as required by PREVENT Duty Guidance for England and Wales.

7. **Report**
   - If I am aware of anyone trying to misuse technology, I will report it to a member of staff.
   - I will speak to a staff member if something happens to either myself or another user which makes me feel worried, scared or uncomfortable.
   - I know that people I meet online may not be who they say they are. If someone online suggests meeting up, then I will report it to a staff member or parent.

Failure to adhere to the terms of the AUP

Non-compliance with the Acceptable Use Policy may result in **disciplinary action** under relevant student conduct policies and illegal activity will be referred to the relevant authorities or external agencies such as the Police.

Users are expected to respect the college's systems and equipment, and misuse may result in revoked access rights.

Related WSFC/Trust Policies and Procedures

- Student code of conduct
- Online Safety Policy and Procedures
- Safeguarding (including Child Protection) Policy
- Anti-Bullying and Harassment Policy and Procedures

Further information

For further information about keeping safe online please visit:

- www.saferinternet.org.uk
- www.thinkuknow.co.uk
- www.childnet.com
- www.childline.org.uk