WINCHESTER
COLLEGE

Winchester College
Pupil Acceptable Usage Policy

Overview

The intentions of publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Winchester College's established culture of openness, trust, and integrity. Winchester College is committed to protecting employees, pupils, and partners from illegal or damaging actions by individuals either knowingly or unknowingly. It is the responsibility of every individual to know these guidelines and to conduct their activities accordingly. All pupils are required to comply with this policy when using digital devices where the culture or reputation of Winchester College is put at risk.

For the avoidance of doubt, the term digital device applies equally to all electronic devices or computers in use by pupils. This policy is subject to alteration as circumstances dictate everyone is expected to use the facilities provided in a reasonable and responsible manner and behave in a way to permit everyone to work to their best advantage.

In cases where the pupil gives rise to safeguarding concerns the matter with be dealt with under the school's child protection procedures and safeguarding policy.

This policy is designed for general usage and is not a comprehensive list of what is and what is not acceptable. All use should be consistent with the school rules, the Winchester Code and the Online Safety and Counter Cyber Bullying Policy and consistent with the rules regarding courtesy and good behaviour.

General Rules

- The purpose of this policy is to outline the acceptable use of computer equipment at Winchester College. These rules are in place to protect the pupils, employees, and Winchester College. Inappropriate use exposes Winchester College to risks including virus attacks, compromise of network systems and services and legal issues.

- Winchester College's proprietary information stored on electronic and computing devices remains the property of Winchester College.

- For security and network maintenance purposes, authorized individuals within Winchester College may monitor equipment, systems, and network traffic at any time.

- System and user-level passwords must comply with the Winchester College Password Policy. Providing access to another individual's account either deliberately or through failure to secure its access is prohibited.

- All computing devices must be secured. Digital devices are enrolled with Winchester College security systems and are prohibited from being removed without consent from the Winchester College IT department.

- In all communications including content shared online will be polite and respectful of others and use appropriate language and refrain from swearing and vulgarities.

- Using photographic or audio material of any kind to bully harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

- You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Winchester College's proprietary information.

- You must not attempt to circumvent Winchester College's IT security systems, including content filters and installation of software that avoids these security systems.

- For security and network maintenance purposes, authorized individuals within Winchester College may monitor equipment, systems, and network traffic at any time.

- Winchester College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

- Unauthorized copying of copyright material including but not limited to the digitation and distribution of copyrighted sources and the installation of any copyrighted software for which Winchester College or an individual does not have an active licence is strictly prohibited.

- You have a responsibility to maintain your Winchester College accounts and must not reveal your account information passwords or allow others access to your account.

- I confirm that there is no harmful content downloaded onto any device I bring into the school, and I will not download any harmful content onto my device via any method that bypasses the School's filtering and monitoring systems.

Counter Cyber bullying
Cyberbullying includes sending or posting harmful or upsetting text, images, or other messages, using the internet or any form of digital device or other communications. This can include threats intimidation harassment defamation, exclusion or peer rejection impersonation and unauthorised publication of private information or images.

Computer Misuse Act
The unauthorised use of computers is a criminal offence. The Computer Misuse Act of 1990 formalises this and explains the different offences and penalties.

Non-Compliance
Any pupil found to have violated this policy may be subject to disciplinary action up to and including exclusion from the school.