WESTERFIELD
COLLEGE

WC18 - IT Policy

College Policy	
Status	Draft
Document Reference No	WC18
Document Title	IT Policy
Version	Version 1
Last Updated	27th January 2024

Information Classification: Private
Status: Draft

Contents

Introduction

This IT Policy outlines the acceptable use, management, and security of IT resources at Westerfield College to ensure a safe, productive, and legally compliant environment for students, staff, and other authorised users. Adherence to this policy is mandatory for all users.

Scope

This policy applies to:

All users of the college's IT resources, including students, staff, contractors, and visitors.

All devices, networks, software, and services provided or authorised by the College.

Both on-campus and remote access to College IT resources.

Acceptable Use

General Principles

IT resources must be used responsibly, ethically, and legally.

Activities should align with the College's educational, administrative, and research objectives.

Prohibited Uses

Accessing or sharing illegal, offensive, or inappropriate content.

Engaging in cyberbullying, harassment, or any behaviour that undermines the dignity of others.

Unauthorized access to or modification of data, accounts, or systems.

Using IT resources for personal financial gain, commercial purposes, or political activities without explicit authorisation.

Personal Use

Limited personal use of IT resources is permitted, provided it does not:

Interfere with academic or work responsibilities.

Breach this policy or any applicable laws.

Consume excessive resources or bandwidth.

User Responsibilities

Account and Password Management

Users must keep their login credentials confidential and must not share them.

Passwords must meet the College's security standards and be updated regularly.

Device Security

All devices accessing College IT resources must be protected with up-to-date antivirus software and security patches.

Users are responsible for the security of their own personal devices when connecting to the College's network.

Data Protection

Users must comply with the UK Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Sensitive data must be securely stored, transmitted, and disposed of following the College's Data Protection Policy.

Network and Internet Usage

The College's network must not be used to download, upload, or share copyrighted material without proper authorisation.

Streaming or downloading large files for non-academic purposes is discouraged to avoid excessive bandwidth consumption.

Users must not attempt to bypass network security measures or access restricted areas.

Monitoring and Privacy

The College reserves the right to monitor the use of IT resources to ensure compliance with this policy, detect security breaches, and maintain system performance.

Monitoring will be conducted in accordance with UK laws, including the Regulation of Investigatory Powers Act 2000.

Software and Licensing

Only software authorised by the College may be installed on College-owned devices.

Users must not install, copy, or distribute software without proper licensing.

Cybersecurity

Users must report any suspected security incidents, such as phishing attempts or malware infections, to the IT Support Team immediately.

The College will provide regular cybersecurity awareness training to all users.

Breaches of Policy

Any breach of this policy may result in disciplinary action in line with the College's disciplinary procedures.

Legal action may be taken in cases of illegal activity.

Contact Information

For questions or assistance regarding this policy, please contact:

IT Support Team: [email address/phone number]

Data Protection Officer: [email address/phone number]

Policy Review

This policy will be reviewed annually by the Academic Board unless there are internal or legislative changes necessitating an earlier review.

Version History

No	Revised on	Version	Changes	Approved by	Date of Approval	Revised by