



# Staff Acceptable Use of Technologies Policy

## Introduction

The purpose of this policy is to establish clear expectations regarding the acceptable use of technology by staff within our Alternative Provision. It aims to safeguard both the Alternative Provision's digital resources and the integrity of our educational environment, while aligning with the 2014 National Curriculum in England and the expectations set forth by Ofsted.

## Purpose of the Policy

This policy serves to:

- Promote the responsible use of technology within the Alternative Provision.
- Protect the Alternative Provision's digital infrastructure and reputation.
- Ensure compliance with legal and regulatory requirements.
- Provide guidance on the use of personal devices on the premises.

## Scope

This policy applies to all staff members, including teaching and non-teaching staff, consultants, volunteers, and any other individuals who have access to the Alternative Provision's technology resources.

# Acceptable Use Guidelines

## General Use

- Staff are expected to use technology in a manner that supports the educational mission of the Alternative Provision, ensuring that all online interactions are professional and respectful.
- All users must comply with the Alternative Provision's code of conduct and mission statement when using any form of technology.
- Staff must not engage in any activity that could harm the reputation of the Alternative Provision, including the transmission of inappropriate content or harassment via digital means.

## Internet and Email Use

- Staff must use the Alternative Provision's email system and internet services for educational purposes and Alternative Provision-related communication only.
- Personal use of the internet should be minimal and should not interfere with the professional responsibilities of staff or disrupt the learning environment.
- Staff should not access websites that are illegal, offensive, or inappropriate (e.g., those that promote violence, hate speech, bullying, or any form of discrimination).
- Employees must be vigilant regarding the content of emails and attachments, ensuring that they do not open files or links from unknown sources to protect the Alternative Provision from cybersecurity threats.

## Social Media Guidelines

- Staff must remember that they represent the Alternative Provision at all times, including on social media platforms; therefore, professional boundaries must be maintained.
- Communication with students through personal social media accounts is strictly prohibited. Any necessary communication must be conducted through Alternative Provision-approved channels (e.g., school email or educational platforms).
- Staff should not publish any content that relates to students, other staff, or the Alternative Provision without prior approval from a line manager, ensuring that sensitive information is protected.
- Staff are encouraged to review their privacy settings on personal accounts to limit access to non-professional contacts.

## **Device Security**

- All devices (including computers, tablets, and smartphones) must be secured with strong, unique passwords and kept in a secure environment, especially when not in use.
- Staff should not share their passwords with anyone and must log out of accounts when finished, especially on public or shared devices.
- Staff must report any suspicious or unusual activity related to Alternative Provision technology immediately to the IT department.
- Personal devices used on Alternative Provision premises must have up-to-date antivirus software and security features.

## **Use of Personal Devices**

- Staff wishing to use personal devices for Alternative Provision work must obtain prior approval from the administration.
- Personal devices must adhere to the same security measures as Alternative Provision-owned devices and should only access Alternative Provision data over secure networks (e.g., via VPN).
- Staff should be aware that data accessed through personal devices may still be subject to monitoring by the Alternative Provision's IT department.

## **Data Protection and Confidentiality**

- Staff must adhere to the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) regarding the handling and storage of personal data.
- Sensitive information about students, staff, parents, and the Alternative Provision must not be shared or discussed outside of Alternative Provision-related contexts.
- All documents and files containing personal data must be stored securely (e.g., on password-protected drives) and deleted when no longer required.

## **Training and Compliance**

- Staff will participate in mandatory training sessions on acceptable use of technology, data protection, cybersecurity, and digital safeguarding annually, with additional sessions as needed.
- Staff are responsible for staying informed about changes in technology and this policy.

- Breaches of this policy will result in disciplinary action, in line with the Alternative Provision's disciplinary procedures which may include warnings, suspension, or termination of employment.

## Monitoring and Review

- The Alternative Provision reserves the right to monitor technology usage to ensure compliance with this policy, including reviewing internet history and inspecting devices if necessary.
- This policy will be reviewed annually, or sooner if necessary, to ensure it is up to date with technological advances and changes in legislation.

## Expectations based on the Most Recent Ofsted Framework

The most recent Ofsted framework highlights several key expectations that our technology use policy aims to support:

1. **Quality of Education:** The application of technology should elevate the quality of education, facilitating effective teaching and learning practices.
2. **Behaviour and Attitudes:** Staff members must model appropriate use of technologies to foster a positive and respectful learning environment, contributing positively to student behaviour.
3. **Personal Development:** Encourage responsible and safe digital citizenship among students by providing staff with the guidance and tools to promote good online practices.
4. **Leadership and Management:** The implementation of this policy demonstrates strong leadership through clear guidelines that protect both staff and students, aligning with the strategic aims of the Alternative Provision.

This policy aims to reflect the values of our Alternative Provision while ensuring compliance with the standards set by Ofsted, thereby fostering an exemplary educational environment conducive to effective learning and teaching.

Written and agreed by: Vanessa Brooks, Lorraine Bunney, Peter Cooper

Date: April 2026

Date of next Review: April 2027