

THE HUB EDUCATIONAL SERVICES CIC

STAFF ACCEPTABLE USE OF TECHNOLOGIES POLICY

Written: April 2026 **Review Date:** April 2027

Introduction

The Hub Educational Services CIC recognises that technology plays an essential role in teaching, learning, communication, and safeguarding. This policy establishes clear expectations for the acceptable use of technology by staff within our Alternative Provision. Its purpose is to protect pupils, staff, and the organisation by ensuring that digital tools are used responsibly, professionally, and safely. The policy aligns with the National Curriculum, Ofsted expectations, the Online Safety Act 2023, and the safeguarding requirements set out in Keeping Children Safe in Education.

Technology is a powerful educational resource, but it also carries risks. Staff must therefore use digital tools in a way that upholds the integrity of our provision, protects sensitive information, and models safe and appropriate behaviour for pupils. This policy outlines how staff should use devices, internet services, email, social media, and personal technology while working at The Hub.

Purpose of the Policy

The purpose of this policy is to promote responsible and professional use of technology across the provision. It aims to protect our digital infrastructure, uphold our reputation, and ensure compliance with legal and regulatory requirements, including data protection legislation. It also provides guidance on the use of personal devices on site, ensuring that staff understand their responsibilities when accessing or storing school-related information.

The policy supports a safe digital environment where staff can use technology effectively while maintaining high standards of conduct and safeguarding.

Scope

This policy applies to all individuals who use The Hub's technology resources, including teaching staff, non-teaching staff, consultants, volunteers, and any other adults who have access to our digital systems. All staff are expected to follow this policy consistently, regardless of their role or level of experience.

Acceptable Use Guidelines

General Use

Staff are expected to use technology in ways that support the educational mission of The Hub and uphold our values. All digital interactions must be professional, respectful, and consistent with our code of conduct. Staff must avoid any activity that could harm the reputation of the provision, including the transmission of inappropriate content, harassment, or behaviour that undermines trust or professionalism.

Technology should be used to enhance teaching, support pupils, and contribute positively to the learning environment. Staff must remain mindful that their digital behaviour reflects on the organisation and must therefore act with integrity at all times.

Internet and Email Use

The Hub's internet services and email system exist primarily to support teaching, learning, communication, and operational tasks. Staff should use these systems for professional purposes and ensure that personal use is minimal, appropriate, and does not interfere with their responsibilities.

Staff must not access websites that are illegal, offensive, discriminatory, or inappropriate. This includes sites that promote violence, hate speech, bullying, extremism, or any form of exploitation. Staff must also exercise caution when opening emails or attachments, particularly from unknown sources, to protect the provision from cybersecurity threats such as malware or phishing attempts.

All communication through The Hub's email system must be professional, accurate, and respectful. Staff must remember that emails may be subject to monitoring and may be disclosed in safeguarding or legal contexts.

Social Media Guidelines

Staff must maintain professional boundaries at all times, including on social media platforms. They represent The Hub both inside and outside the workplace, and their online behaviour must reflect this responsibility. Communication with pupils through personal social media accounts is strictly prohibited. Any necessary communication must take place through approved channels such as school email or designated educational platforms.

Staff must not publish content relating to pupils, colleagues, or the provision without prior approval from a line manager. This includes photographs, videos, comments, or any information that could identify individuals or compromise confidentiality. Staff are

encouraged to review privacy settings on personal accounts to limit access to non-professional contacts and reduce the risk of inappropriate interactions.

Device Security

All devices used for work purposes must be kept secure. Staff must use strong, unique passwords and ensure that devices are stored safely when not in use. Passwords must not be shared, and staff must log out of accounts when using shared or public devices.

Suspicious activity, unusual behaviour on devices, or potential security breaches must be reported immediately to the IT department. Staff using personal devices on site must ensure that these devices have up-to-date antivirus software and appropriate security features to protect school data.

Use of Personal Devices

Staff may use personal devices for work only with prior approval from the administration. Personal devices must meet the same security standards as school-owned devices and may only access school data through secure networks, such as a VPN. Staff should be aware that data accessed on personal devices may be subject to monitoring in line with safeguarding and data protection requirements.

Data Protection and Confidentiality

Staff must comply with the Data Protection Act 2018 and UK GDPR when handling personal data. Information relating to pupils, staff, parents, or the provision must be stored securely, accessed only when necessary, and shared only in appropriate professional contexts. Sensitive information must never be discussed outside of work-related settings.

Documents containing personal data must be stored on secure, password-protected systems and deleted when no longer required. Staff must follow The Hub’s data protection procedures at all times to ensure confidentiality and compliance with legal obligations.

Training and Compliance

All staff participate in mandatory annual training on acceptable use of technology, data protection, cybersecurity, and digital safeguarding. Additional training is provided when necessary, particularly when new systems or risks emerge. Staff are responsible for staying informed about updates to this policy and changes in technology that may affect their responsibilities.

Breaches of this policy may result in disciplinary action in accordance with The Hub’s disciplinary procedures. Depending on the severity of the breach, consequences may include warnings, suspension, or termination of employment.

Monitoring and Review

The Hub reserves the right to monitor staff use of technology to ensure compliance with this policy. This may include reviewing internet history, inspecting devices, or monitoring email activity where necessary. Monitoring is carried out in accordance with safeguarding, data protection, and employment legislation.

This policy is reviewed annually, or sooner if required, to ensure that it remains up to date with technological developments, legislative changes, and Ofsted expectations.

Alignment with Ofsted Expectations

The most recent Ofsted framework emphasises the importance of technology in supporting high-quality education, modelling positive behaviour, and promoting responsible digital citizenship. Staff are expected to use technology in ways that enhance teaching and learning, contribute to a respectful and safe environment, and support pupils' personal development.

Leadership and management are strengthened when clear guidelines are in place to protect staff and pupils. This policy demonstrates The Hub's commitment to safeguarding, professionalism, and effective digital practice.

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

Date: April 2026

Next Review: April 2027