HORIZONS EDUCATION TRUST

Acceptable Use of ICT Policy

October, 2024

POLICY ISSUE CONTROL

POLICY TYPE:	Statutory, Mandatory
OWNER:	Operations Manager
AUTHOR: **IN CONSULTATION WITH:**	Operations Manager
APPROVED BY:	Interim CEO
TRUST BOARD APPROVAL:	Full Board, October 2024
RELEASE DATE:	October 2024
REVIEW:	October 2025

	Document Control
Date reviewed: Sept 2024 Date of next review: Sept 2025 Reviewer: Jon Panther (Operations Manager) Date of ratification by Governing Board: TBC	Policy re-written to simplify its contents

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 **Purpose**: This policy outlines the acceptable use of the Trust and its academies' digital technology resources and systems, hereafter known as Horizons Education Trust (HEdT). All staff members are required to adhere to this policy to ensure compliance with UK legislation, including the latest guidance under "Keeping Children Safe in Education" (2024) and UK GDPR.

1.2 **Scope**: The policy applies to all employees, contractors, volunteers, and others who have access to HEdT IT resources, both within and outside HEdT premises.

1.3 **Professional Use**: Any computer, laptop, or other digital technology resource provided by HEdT is intended solely to support professional responsibilities. These resources should only be used for professional purposes or other uses deemed 'reasonable' by a member of the senior management team.

2.0 DATA PROTECTION

2.1 **Compliance with Data Protection Laws**: Staff must adhere to the UK GDPR and the Data Protection Act 2018. Any personal data related to staff or pupils that is held within the school's systems must be kept private and confidential unless disclosure is required by law or directed by an appropriate authority.

2.2 **Data Handling**: All documents, data, and other information must be saved, accessed, and deleted in accordance with the HEdT's data security and confidentiality protocols. This includes ensuring that sensitive information is encrypted when transmitted electronically and is not accessible by unauthorised persons.

2.3 **Passwords**: Login passwords must be strong, regularly updated, and kept confidential. Passwords should not be shared except where necessary for technical support, and only with the approval of senior management.

3.0 PROHIBITED USE

3.1 **Inappropriate Content**: The use of electronic media to view, transmit, retrieve, or store content that is:

- Discriminatory or harassing
- Derogatory to any individual or group
- Obscene, sexually explicit, or pornographic
- Defamatory or threatening
- In violation of any software license
- Engaged in any illegal activity or contrary to the school's policies or interests is strictly prohibited.

3.2 **Personal Use**

3.2.1 **Limited Personal Use**: HEdT's digital technology resources are primarily for educational and professional use. Limited, occasional personal use is permissible if it does not interfere with the educational use or occur during contact hours.

3.2.2 **Personal Devices**: Personal ICT equipment, including mobile phones, must not be used to contact students, parent/carers, or guardians without prior authorisation from the Headteacher. The use of personal devices to take photographs or engage in email or social media concerning school matters is strictly prohibited unless specifically approved by the Headteacher.

3.2.3 **Social Media**: Staff must not access social networking sites (e.g., Facebook, Twitter) using the HEdT internet connection during working hours. No reference should be made to HEdT on any social networking site.

4.0 ACCESS TO EMPLOYEE COMMUNICATIONS AND FILES

4.1 **Monitoring**: HEdT reserves the right to monitor and log electronic activities to detect any patterns of misuse. Electronic information, including emails and other communications, may be reviewed to ensure compliance with legal requirements and academy policies.

4.2 **Privacy**: Staff should not assume that their electronic communications are private. Sensitive information sent outside the HEdT domain should be transmitted securely and in compliance with data protection laws.

4.3 **Pupil Data**: Pupil data should not be transmitted over the internet or via email without appropriate encryption and consultation with senior management to ensure compliance with information-sharing protocols.

4.4 **Business Continuity**: HEdT may access an employee's electronic files and communications to ensure business continuity during long-term absence or upon resignation.

5.0 SOFTWARE

5.1 **Software Installation**: Only software that is licensed and approved by HEdT may be installed on HEdT equipment. Staff must seek advice and permission from the Headteacher before downloading or installing any software. Violations may result in disciplinary action.

6.0 SECURITY AND RESPONSIBILITY

6.1 **Security Measures**: All employees are responsible for maintaining the security of academy equipment. This includes:

- Securing laptops and other equipment at the end of each school day
- Reporting any loss or damage to the Headteacher immediately
- Keeping login details confidential
- Logging out and shutting down computers at the end of the day
- Never allowing pupils to access staff devices

6.2 **Device Use**: Pupils should not be permitted to use devices logged in under a staff account or access designated administration machines.

7.0 APPROPRIATE USE

- **Professional Conduct**: Staff must use HEdT's digital technology resources only for professional purposes or reasonable uses as approved by senior management or the governing Body.

8.0 PROHIBITED ACTIONS:

8.1 Staff May Not Engage In:

- Monitoring or intercepting files or communications of others without authorisation
- Hacking or attempting to access systems or accounts they are not authorised to use
- Breaching security measures
- Sending communications that attempt to hide the sender's identity
- Copying or distributing copyrighted materials without permission

8.2 Use of Work Devices Outside School

- **External Use**: When using HEdT devices outside the premises, staff must ensure that the devices remain secure and password protected. The installation of unauthorised software is prohibited, and external storage devices containing pupil or staff data must not be taken off-site without encryption.

8.3 Participation in Online Activity

- **Social Networking**: While staff may participate in social networking in their own time, they are strongly advised against it. If they choose to do so, they are solely responsible for any inappropriate content that becomes public. Such actions could lead to disciplinary procedures, including dismissal.
    - You must not accept "friend requests" from any children or parent/carers over personal social networking sites, unless the person is known outside of their job role. If the latter is the case, the Headteacher, or central team line manager, must be made aware of the relationship.

- **Professional Boundaries**: Staff must ensure that their personal online activities do not compromise their professional role. They must not represent the HEdT online without explicit authorisation from the Headteacher.

- **Content Restrictions**: Staff must not post images or content that could be linked to their professional role or compromise HEdT's reputation.

8.4 Mobile Phones

- **Use in School**: Personal mobile phones are prohibited in areas accessible by students. Phones should be stored securely and only used before or after school hours, or during scheduled breaks.

8.5 Media Publications

- **Parental Consent**: Written permission from parent/carers must be obtained before publishing photographs or names of pupils. All media content created within the Trust is the property of HEdT, and must not be published without the consent of a member of the senior management team.

9.0 POLICY LINKS

Related Policies: This policy should be read in conjunction with other relevant HEdT policies, including:

- Safeguarding and Child Protection Policies
- Keeping Children Safe in Education (2024)
- Working Together to Safeguard Children
- Whistleblowing Policy
- PREVENT Training
- Equalities Policy
- E-Safety Policy
- Data Protection Policy

10.0 DECLARATION

Acceptance: All staff and volunteers must sign the agreement form enclosed to confirm their understanding and acceptance of this policy within 5 working days of its issue.

Employee Acceptance Form

I confirm that I have read and understood the ICT Acceptable Use Policy

I understand that not following this policy is a breach of my employment contract and of the Staff Code of Conduct.

Signature of Employee:

Print Name:

Date:
