Parents Acceptable Usage Policy

Reviewed June 2024

The Stour Academy Trust

Introduction

1.1 This Policy provides the guidelines of acceptable use of Information Communications Technology (ICT) equipment and facilities within The Stour Academy Trust. ICT is seen as beneficial to all members of the Trust in supporting learning, teaching, research, administration, and approved business activities of the Trust. The Trust's ICT Facilities provide several integral services and, therefore, any attempt to misuse a computer system could cause significant disruption to other users at the Trust. This could also lead to a breach of the data protection rights of individuals, resulting in harm to that individual and the Trust.

1.2 The purpose of the Acceptable Use Policy is not to impose restrictions that are contrary to established culture of openness, trust, and integrity within the Trust. This policy is designed to protect all authorised users from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.3 All Users, including but not limited to Directors, staff, and pupils using the Trust's Information Technology and Systems must ensure that they have read this Policy before commencing to its information and communication technology. Failure to do so will not be accepted as a mitigation factor should a problem arise during employment or period of study.

2. Definitions

2.1 *"Trust"* means The Stour Academy Trust.

2.2 *"ICT Device"* means any laptops, tablets, telephones, smartphones, desktop computer, console, printer, speaker, camera, or other electronic equipment that could be used for the carrying out of Trust business or the processing or storing of information.

2.3 *"ICT Facilities"* means all devices, facilities, systems, and services including, but not limited to, network infrastructure, ICT Devices, software, websites, web applications or services and any device, system or service which may become available in the future which is provided as part of the ICT service.

2.4 *"Users"* means directors, staff, pupils, trainees, volunteers, temporary guests, and all other persons authorised by the Trust to use the ICT Facilities.

2.5 *"Personal use"* means any use or activity not related to the users' employment, study, or purpose.

2.6 *"Authorised Personnel"* means employee(s) authorised by the Trust to perform systems administration and/or monitoring of the ICT Facilities. This includes the CEO, COO, and IT personnel.

2.7 *"Materials"* means files and data created using the ICT Facilities including but not limited to documents, photographs, audio, video, printed output, web pages, social networking sites, bulletin boards, newsgroups forums and blogs.

3. Policy Statement

3.1 The Trust's ICT Facilities should only be used to support learning, teaching, research, administration, and approved business activities of the Trust. The ICT Facilities must not be used for personal commercial, political, charitable, and other such activities unless expressly authorised by the Trust.

3.2 The Trust employs various measures to protect the security of its computing resources and of its user accounts. Users should be aware that the Trust cannot guarantee such security. Users should therefore engage in safe computing practices by establishing adhering to the Trust's Information Security Policy at all times, backing up files, and promptly reporting any misuse or violations of this policy.

3.3 All devices that use the ICT Facilities, and that are capable of supporting software updates, security updates and automatically updating anti-virus products, must be configured to perform such updates.

3.4 Users' accounts and passwords must not be shared with anyone. Users are responsible for the security of their passwords, accounts and setting account and file permissions. Disclosure of account or password information may result is disciplinary action.

3.5 Users must abide by all applicable laws and Trust policies to protect the copyrights and intellectual property rights of others. Copyrighted works may include texts, cartoons, articles, photographs, songs, videos, software, graphics, and other materials. This includes the use of the internet, as many of the materials available through the internet are protected by copyright. It is the responsibility of the user to assume that materials found upon the internet are copyrighted unless the materials contain an express disclaimer to the contrary. Users must obtain permission of the creator or publisher to copy or use software or other copyrighted materials written or created by others and must abide by contracts and agreements controlling installation and use of such software and other materials.

3.6 Users' use of the ICT Facilities must be in an ethical and legal manner and in accordance with Trust policies and procedures. sage of the system to harass, defame, or invade the privacy of others, or to send or receive obscene materials, is not allowed, and may result in disciplinary action under policies controlled by the Trust or prosecution under applicable laws.

3.7 Pupils should not use ICT facilities for personal use under any circumstances.

3.8 The Trust will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of ICT Facilities.

4. Unacceptable Use

4.1 The Trust reserves the right to block, disconnect, remove devices, or otherwise prevent what it considers to be unacceptable use of its ICT Facilities. Unacceptable use includes, but is not limited to:

4.1.1 All actions or activities that are illegal or in conflict with the Trust's policies, procedures, processes and regulations or which breach contracts or policies applied to the Trust by third party through a valid service contract or agreement.

4.1.2 Using the ICT Facilities for access, creation, modification, storage, download, hosting, or transmission of material that could be considered pornographic, offensive, obscene, or otherwise inappropriate, or for placing direct or indirect links to websites which publish or host offensive or inappropriate material.

4.1.3 Publishing materials or making statements which the Trust may deem to be advocating illegal activity, or threatening, or harassing, or defamatory, or bullying or disparaging of others, or abusive, or libellous, or slanderous, or indecent, or obscene, or offensive or promotes unlawful discrimination, breaches copyright or otherwise causing annoyance, or inconvenience.

4.1.4 Unauthorised production, distribution, copying, selling, hiring, performing of copyrighted material including, but not limited to, digitisation and distribution of computer software, television, radio, streaming services, websites, photographs, magazines, books, music or any copyrighted sources and installation of any copyrighted software for which the Trust does not have an active licence or explicit permission of the copyright owner, is strictly prohibited.

4.1.5 Authoring or sending any form of electronic communications or messages, including, but not limited to, videos, chats, messages and/or emails that were unsolicited and may be considered inappropriate, junk, "chain letters", "Ponzi", hoax warnings or advertising, and that do not correctly identify you as the sender, or messages which appear to originate from another person.

4.1.6 Unauthorised recording, "screenshotting," capturing, photographing or any other means of observing and/or documenting the *Materials* of an ICT device, without prior notification and agreement.

4.1.6 Unauthorised transmission, distribution, discussion, or disclosure of information gained through a user's presence within the Trust or using ICT Facilities.

4.1.7 Connecting any non-approved ICT device, system, or service (including wireless access points) to Trust networks or setting up any network services, without the explicit or delegated permission from Authorised Personnel.

4.1.9 Unauthorised access (or attempted unauthorised access) to any ICT Facilities provided by the Trust.

4.1.10 Allowing, inciting, encouraging, or enabling others to gain or attempt to gain unauthorised access to the ICT Facilities.

4.1.11 **Causing any damage to ICT Facilities such as cracked screens, including through the consumption of food or drink, or moving or removing such facilities without authorisation. The Trust reserves the right to charge for any damage caused.**

4.1.12 Attempting to modify, alter or in any way interfere with ICT facility security controls, hardware or software, configurations, settings, equipment, data files or websites without the written authorisation or delegated permission from Authorised Personnel.

4.1.13 Introduction of unauthorised and/or malicious software or programs into the ICT Facilities, including, but not limited to unlicensed software, viruses, worms, Trojan horses, or logic bombs; by downloading, creating, or using any program, tool or item of software designed to monitor damage, disrupt, or interfere with the functioning of ICT Facilities, user accounts or data.

4.1.14 Effecting security breaches or disruptions of network communication, including, but not limited to, accessing, or modifying data (or data headers) of which the user is not an intended recipient or logging into an ICT system or service, or account, that the user is not expressly authorised to access. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.

4.1.15 Executing any form of network monitoring including any data capture, port scanning or security scanning without written authorisation or delegated permission from Authorised Personnel.

4.1.16 Registering for any system or service, including, but not limited to, social media accounts, web applications, domain names, which includes the name of the Trust or any similar name, or abbreviation that may mislead the public into believing that the domain name refers to the Trust.

4.1.17 Acting in any way that directly or indirectly causes disruption to others' use of Trust ICT Facilities or using ICT Facilities to disrupt or deny the use of ICT Facilities of third parties at any time.

Home Usage

In alignment with our commitment to enhancing learning beyond school premises, KS2 pupils may take school-issued iPads home. This addendum to our Acceptable Usage Policy ensures that both parents and pupils understand their responsibilities and the expectations for home usage of these devices.

Guidelines for Home Use

Purpose of Use: iPads must be used primarily for educational purposes, following the same usage guidelines as in school. Non-educational use should be minimal and not interfere with academic activities.

Security Measures: Devices should be secured with passwords that are not shared outside the immediate family. Parents are responsible for monitoring the usage of these devices to ensure compliance with our safety protocols.

Content Restrictions: Just as at school, the use of inappropriate or unauthorised apps and websites is strictly forbidden. Parents should supervise and ensure that content accessed is appropriate and educational.

Parental Responsibilities

Monitoring: Regular checks should be performed by parents to ensure that the device is being used appropriately. This includes reviewing browsing history and app usage.

Reporting Issues: Any technical or compliance issues must be reported to the school immediately. This includes loss of device, exposure to inappropriate content, or device malfunction.

Physical Care: Parents are responsible for the physical care of the iPad when it is out of school, ensuring that it is handled gently and kept away from potential damages such as liquids or falls.

Consequences of Misuse

Misuse of the device at home will be treated with the same seriousness as misuse at school. Consequences may include revocation of home usage privileges, disciplinary action, and possible financial responsibility for damages.

Remote Learning

5.1 Online collaboration is essential for remote learning providing increased opportunities to maintain the connection between school and home.

5.2 Users engaging, participating or otherwise connected to the ICT Facilities are expected to abide by the Acceptable Use Policy, and all other applicable policies, including but not limited to the Remote Learning Policy.

6. ICT Monitoring

6.1 The Trust will monitor the usage of any or all ICT Facilitates and has access to reports on any internet sites that have been visited. Such monitoring will be performed in compliance with this policy in line with DFE filtering and monitoring legislation/ expectations

6.2 Teachers will check all equipment regularly for correct usage and report anything they find unsuitable via regular 'Tech Checks'

7. Monitoring & Review

7.1 This policy will be reviewed every 2 years and may be subject to change

Acknowledgment

Parents and pupils are required to consent indicating that they have read, understood, and agreed to adhere to these guidelines. Compliance is mandatory to maintain the privilege of home usage of school devices.