The
Three
Rivers
Learning Trust

Name of Policy	**ICT Control & Security**
Policy Number	**NS13**
The Three Rivers	
Named Person(s)	**ICT North**
Review Committee	**Board**
Last review date	Autumn 2019
Next review date	Autumn 2022

Usage Guidance

1.0 Overview

The Three Rivers Learning Trust intentions for publishing an ICT Control and Security Guidance are not to impose restrictions that are contrary to the Trusts established culture of openness, trust and integrity. Network Management is committed to protecting the Trust's employees, partners and the students from illegal or damaging actions by individuals, either knowingly or unknowingly.

Network and Cloud based systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of The Three Rivers Learning Trust. These systems are to be used for business purposes in serving the interests of the schools, and of our staff and pupils in the course of normal operations.

Effective security is a team effort involving the participation and support of every The Three Rivers Learning Trust employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at The Three Rivers Learning Trust in relation to keeping people and systems safe. These rules are in place to protect the employee and The Three Rivers Learning Trust. Inappropriate use exposes The Trust to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, students and other workers at The Three Rivers Learning Trust, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by The Three Rivers Learning Trust.

4.0 Policy

4.1 General Use and Ownership

1. While The Trust's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the school systems remains the property of The Three Rivers Learning Trust. Because of the need to protect The Trust's network, it cannot guarantee the confidentiality of information stored on any network device belonging to The Three Rivers Learning Trust.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
3. Network Management recommends that any information that users consider sensitive or vulnerable be encrypted, or require a network username and password.
4. For security and network maintenance purposes, authorised individuals within The Three Rivers Learning Trust may monitor equipment, systems and network traffic at any time, per the data protection act 1998.
5. The Three Rivers Learning Trust reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Employees should take all necessary steps to prevent unauthorised access to confidential or sensitive information. Examples of confidential information include but are not limited to: school private documents, school strategies, specifications, staff and student lists, student data, and research data.
2. Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every 6 months as a minimum, but immediately if a user thinks their password may have been compromised.
3. All Staff workstations and portable devices should be secured with a password with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows Operating Systems) when the host will be unattended.
4. Information contained on portable devices is especially vulnerable. Special care should be exercised. Portable devices should not be shared with users outside of the Trust. If devices are shared, then users should log off and secure the device when finished or passing to another user.
5. All devices that are connected to The Three Rivers Learning Trust Network and/or Cloud based services, shall be continually executing approved up to date virus-scanning software.
6. Employees must use extreme caution when receiving email attachments from unknown senders, which may contain viruses, email bombs, Trojan horse code, or other malicious code. Emails of this sort should be deleted.
7. All Portable Windows computers should be secured with Bitlocker encryption before leaving the premises.
8. Bitlocker Encryption keys must be backed up centrally to the IT technical departments shared drive.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting services).

Under no circumstances is an employee of The Three Rivers Learning Trust authorised to engage in any activity that is illegal under national or international law while utilising The Three Rivers Learning Trust-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by The Three Rivers Learning Trust.
2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which The Three Rivers Learning Trust or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs and/or other malicious code.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when using equipment or accessing Trust systems at home.
5. Using a The Three Rivers Learning Trust device to actively engage in procuring or transmitting material that would be deemed inappropriate within the Trust’s environment. This includes material of a sexual or violent nature, material containing extreme views or material which could negatively affect the health and well being of staff or students.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

7. Port scanning or security scanning is expressly prohibited unless prior notification to Network Management is made.
8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security.
10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.
11. Automatic blocking of unsolicited peer-to-peer networks will be facilitated in accordance with the learning trusts policies and procedures using the technology available (currently Meraki’s Air Marshal)

4.5 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, whether through language, frequency, or size of messages.
3. Unauthorised use, or forging, of email header or letterhead information.

5.0 BYOD and Chromebooks, iPad’s & other Mobile devices

1. Chromebook devices owned by the learning trust will be restricted to learning trust email accounts, staff should not leave these devices unattended, or logged in for other users (including family members, or colleagues), these devices will be managed by a suitable MDM system (currently Google’s Mobile Device console)
2. iPad devices owned by the learning trust should be secured using a suitable MDM system (currently Meraki) and secured so that they cannot be used outside of the trusts geographical location after a grace period of time (currently 1 hour), also known as Geofencing.
3. All other mobile devices, including laptops owned by the learning trust, will either be managed by either a suitable MDM system, or domain/users policies.
4. Mobile devices used by staff to access email (but not restricted to) should be secured with a pin code, and where applicable managed by a suitable MDM system.
5. Android work profile to be allowed as an opt-in solution with mobile device policy in place to control trust data centrally from the Google Cloud console on personal devices that could be lost or stolen.

6.0 Data Retention and Leavers.

1. Student data will be archived and kept for a reasonable period of time (12 Months) for student alumni, after this period it will be removed from the archive.

2. Staff Data will be transferred to another department member, but all access will be revoked from the current leaving staff member.
3. Google Apps For Education data will only be kept until the start of the new academic year (September).
4. This information will be relayed by assemblies and the student leavers form.