Name of Policy	**ICT Control & Security**
Policy Number	**NS13**
The Three Rivers	
Named Person(s)	**ICT North**
Review Committee	**Board**
Last review date	Summer 2022
Next review date	Summer 2025
Revisions	May 2022: Following a recent Cyber Security Audit, the following amendments/additions have been made to section 4 of the policy: Page 3: New section 4.2 Access Control Page 3: New bullet point added at the start of section 4.3 Page 4: New section 4.4 Passwords Page 6 - 10: New sections added, 4.8 to 4.14

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 judgement 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 Access Control

1. All users, inclusive of suppliers with direct access to the Trust's information technology systems will take all reasonable care to prevent their access to the system being hijacked by an unauthorised person. This includes ensuring that computers are locked or logged off when left unattended and conforming with the organisation's Password Policy.
2. When determining who requires access to information and what they can do with it, the Trust will only grant the privileges required to effectively carry out their job role.
3. When determining who requires access to sensitive information, the Trust will consider who needs access to the data; not who might at some point need access to the data, granting individuals access to highly sensitive documents, rather than groups.
4. The Trust provides access to non-sensitive data by job function or department. This is to simplify the privileges structure and to limit the impact in the event of compromise.
5. Where possible, the Trust always issues unique digital identities to employees and service providers with access to its information technology systems. On most occasions, this is a unique username and password.
6. The Trust will conduct an 'Accounts and Privileges Review' every 6 months.
7. Accounts used to administer the Trust's information technology systems are, where possible, only used for administration purposes. Administrative accounts on operating systems and productivity services will not be used for daily operations.
8. User accounts are provisioned, decommissioned, promoted and demoted by means of submitting a request to the ICT Helpdesk.
9. The Trust maintains a register of all users with special privileges to information systems. Special Privileges are digital identities with a level of access higher than any standard account. This register is known as the Special Privilege Register and is reviewed during the 'Accounts and Privileges Review' every 6 months. Maintaining the Special Privilege Register allows the Trust to provide additional controls to higher risk digital identities.

4.3 Security and Proprietary Information

1. To assure that systems are secure, three key information security principles must be guaranteed, namely confidentiality, integrity and availability. A violation of any of these principles compromises the security of a computer system and such may lead to severe unintended consequences. These principles aim to:
    - make provision for the availability of information where there is a legitimate reason to do so.
    - ensure the integrity of information is always maintained.
    - guide technical and non-technical controls and measures that ensure information is protected from unauthorised access using authentication and authorisation methods
2. 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.

3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. All Portable Windows computers should be secured with Bitlocker encryption before leaving the premises.
9. Bitlocker Encryption keys must be backed up centrally to the IT technical departments shared drive.

4.4 Passwords

1. The Trust always changes default credentials. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.
2. The Trust follows the following principles when creating a new password.

    - Are never obvious (easy for an attacker to guess)
    - Are never commonly used passwords
    - Have never been disclosed in a breach (validated using the HaveIBeenPwned service (haveibeenpwned.com)
    - Are never re-used when a password expires
    - Are never re-used across different accounts

3. The Trust employees and contracted staff will never:

    - Write down their passwords or encryption keys
    - Disclose their password to others

4. Trust staff or technicians will never ask employees or contracted staff for their password.
5. All employees and contracted staff at the Trust will ensure that multi-factor authentication is enabled for all devices and services that support this technology.

4.5. 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.

4.6 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)

4.7 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.

4.8 Anti-Malware

1. All information technology assets of the Trust must have the organisation's designated anti-malware software installed where the software is compatible.
2. 's anti-malware software will be configured to perform:
   - On-access scanning of files and web pages
   - On-access scanning of removable media
   - Scheduled full system scans on a daily basis
   - Daily definition database updates
3. The Trust requires all personal devices used by staff to access its information assets to have at least the operating system's default anti-malware software to be enabled and preferably its designated anti-malware software installed.

4.9 Incident Management and Response

1. The Trust's cyber security incident management and response plan provides guidance on what the school regards to be a cybersecurity incident, including methods of reporting. All suspected information security breaches need to be reported and investigated. All significant security recommendations must be incorporated into the risk action plan. In the case of a significant disruption to the school's information systems, the business continuity plan should be invoked to ensure a systematic, swift and effective recovery process in the best interest of the school.

4.10 System Change Management

1. Changes to the Trust's functional requirements that may call for modifications to existing information systems might affect the information security controls and processes and thus risk management controls may need to be implemented accordingly. Appropriate security provisions need to be taken into account before any significant changes are made to the school's network.

4.11 Patch Management

1. The Trust ensures that all its workstations are running an operating system that is actively supported by the vendor according to its development life cycle. Workstations running retired or legacy operating systems are removed

from service. Automatic updates are enabled for all workstations' operating system, updating at the default frequency defined by the vendor.

2. The Trust aims to install all security patches within 14 days of release and aims to install patches not related to security within 90 days.
3. The Trust will take all reasonable measures to ensure that updates known to be problematic are prevented from being installed until resolved by the vendor.
4. The Trust does not operate unlicensed software and takes all reasonable measures to ensure that it meets all End User Licence Agreement terms.
5. The Trust takes all reasonable measures to ensure that the software it uses is supported by its vendor. There may be occasions where no alternative software is available; in this case the software must be approved and marked as unsupported in theTrust information asset register.

4.12 Ransomware

1. The National Cyber Security Centre's (NCSC) definition reads: *"Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted*."
2. The Trust recognises and acknowledges the threat of ransomware attacks and the severity of the impact on the Trust's computer systems and operations and aims to prepare accordingly. To prepare for and defend against ransomware attacks, the Trust deploys strategies and controls which may include the following:
    - **Data classification** - Not all data is equal and thus data should be classified and stored according to the sensitivity level. The school should be aware of the systems that process and store critical/sensitive data and such must be documented.
    - **Effective backup strategies** - Backup systems are the first port of call in the case of a ransomware attack. Ransomware attacks aim to sabotage recovery operations thus, the school aims to implement effective backup strategies and data recovery operations by:
        - conducting regular backups of data, and most importantly, of critical/sensitive data
        - having offline backups preferably offsite
        - having multiple copies of the same file using different backup systems
        - scanning backup systems for malware where possible, especially before recovery
        - regularly testing data recovery operations
    - **Staff awareness training** - The school conducts regular staff awareness training to educate staff in areas which include but not limited to best security practices, common attack vectors, phishing email attacks, password handling, reporting channels.

- **Patch management** -the Trust follows the patching schedule described in this Policy to reduce an attacker's probability of gaining access through a discovered security vulnerability.
- **Cyber insurance** - Cyber insurance will assist the Trust with recovery costs in the case theTrust suffers a breach.
- **Regular incident management plan rehearsal** - A timely and well-coordinated response to a ransomware attack might lessen the impact.The Trust aims to regularly review and test the incident management plan to ensure that it's up-to-date and that all the pre-defined roles and responsibilities are clearly defined.

3. Network monitoring strategies and suspicious behaviour detection controls are implemented across the Trust's computer systems and networks. This approach aims to implement technology best practices as well as non-technical approaches which may include:

- Ensuring anti-malware software applications are installed and enabled on all endpoints, virus signature databases are always up-to-date and files are set to be scanned on-access.
- Automated suspicious/unusual behaviour event notifications including the deploying a monitored 'honeypot' folder at the top of critical data directories that serves as an early-warning.
- Deploying robust email filtering systems to block, quarantine or flag suspicious emails.
- Reporting of suspicious emails or events by school staff.

4. In the case theTrust is breached, the main aim is to contain the malware to prevent it from spreading to other systems.The Trust follows the NCSC guidelines to help limit the impact:

- Quick disconnection and isolation of infected computers, laptops or tablets from all network connections. If multiple devices are infected, network equipment including routers, switches and wireless access points may also need to be turned off.
- User credentials for user accounts associated with the infected device will be reset
- The latest patches will be applied to non-infected devices
- Infected devices are wiped and rebuilt
- All backup systems must be thoroughly scanned for malware before data recovery operations are commenced.
- Verify that endpoint anti-malware software applications are installed, up-to-date and enabled on all systems.
- Continuous monitoring of network traffic and anti-malware scans to verify if traces of the malware still exist.

5. Lessons learnt are discussed, documented and changes are made to the incident management plan and other internal processes where necessary.
6. In the event that the Trust's backup systems fail and data is unrecoverable, the only option might be to pay and that so being, the Trust follows the National Crime Agency (NCA) and the ESFA's guidance regarding ransomware payments.

7. The Trust will contact the ESFA first to obtain permission to pay any cyber ransom demands.The Trust is fully aware that by making such payments:
   - our computer systems may be more likely to be targeted in the future
   - there is no guarantee that the Trust's data will be returned
   - theTrust will be paying cybercriminals which will likely be funding organised crime.

4.13 Secure Configuration

1. The Trust's IT assets are regularly reviewed to keep them aligned to the school's dynamic functional requirements and any unnecessary or unused services are removed. All default credentials are changed to meet the standard detailed in the school's password policy. The Trust adheres to the 'least privilege' principle which ensures that users are granted the least possible privileges adequate enough to carry out work responsibilities. These principles aim to:
   - Prevent unauthorised users from collecting, copying and modifying data.
   - Prohibit the use of removable media (and other external peripheral devices) where possible, and to scan for malware where use is allowed.
   - Prevent the execution of malicious code.
2. The Trust maintains an asset register which contains a list of approved software applications and hardware. All new software and hardware installations and modifications are approved and continuously monitored and standard users are not permitted to perform any new installations.
3. The Trust ensures least privilege access to standard users which prevents them from installing additional software or creating additional user accounts. Access to systems strictly requires a strong password as detailed in the password policy. All user accounts are reviewed as stipulated in the school's access control policy and unnecessary accounts are removed or disabled.
4. The Trust implements application allow-listing for mobile and tablet devices, which explicitly permits only authorised software from the operating system vendor's 'app store' to be installed and executed on school devices where possible. Where allow-listing is not possible, the installation of new scripts and applications is prevented by restricting user privileges.
5. Automatic execution of code is prohibited. On Windows systems, auto-run is disabled using technical controls.

4.14 Firewalling

1. The Trust always changes default credentials on network boundary firewalls. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.
2. The Trust follows the principles outlined in its Password Policy when changing network boundary firewall passwords.
3. The Trust requires that Network Boundary Firewalls have the following capabilities supported and enabled:

- HTTP and HTTPS proxy
- Gateway antivirus
- Multi-WAN with failover functionality (if multiple WANs are installed)
- Intrusion Prevention System
- Advanced Persistent Threat protection

4. The Trust requires that the host-based firewall is enabled on all network connected endpoints that have such ability.
5. The Trust requires that the host-based firewall, or at least the built-in Windows or Mac OS host-based firewall is enabled on all network connected endpoints that have such ability.
6. The Trust does not allow services that are identified by the NCSC, GCHQ or the Cyber Essentials scheme as vulnerable to be allowed to connect through firewalls. Services that are identified as vulnerable are as follows:

- SMB
- TELNET
- NetBIOS
- tFTP
- RPC
- rLogin
- RSH
- rExec
- HTTP

7. Access to the internet from the Trust Local Area Networks is granted only to devices that require access as an operational necessity. Restriction of access is implemented by a 'Blanket Deny'.
8. The Trust maintains a register of all approved firewall rules permitted on Boundary Firewalls using the built-in access control list on the device, adding clear justification in the description of each rule.

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.