Truro and Penwith Academy Trust

IT ACCESS POLICY v1.0

Threemilestone School

Review Summary

Approved By:	**Trust Board**
Approval Date:	**May 2023**
Next Review Date:	**May 2024**

Table of Content

Truro and Penwith
Academy Trust

IT Access Policy

1. Introduction

1.1. Information security is the protection of information against accidental or malicious disclosure, modification or destruction.

1.2. Information is an important, valuable asset of Truro & Penwith Academy Trust which must be managed with care and all information has a value to Truro & Penwith Academy Trust and our competitors or criminal actors.

1.3. Access controls are put in place to protect information by controlling who has the right to use different information resources and by guarding against unauthorised use. Formal procedures must control how access to information is granted and how such access is changed.

1.4. This policy also mandates a standard for the creation of strong passwords and their protection.

2. Definition, Purpose, Scope and Risks

2.1. Definition

2.1.1. Access control rules and procedures are required to regulate who can access Truro & Penwith Academy Trust's information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Truro & Penwith Academy Trust's information in any format, and on any device.

2.2. Purpose

2.2.1. The purpose of this policy is to prevent unauthorised access to Truro & Penwith Academy Trust's information systems. The policy describes the registration and de registration process for all Truro & Penwith Academy Trust information systems and services.

2.2.2. These policies apply especially to new starters, leavers and those moving roles or responsibilities.

2.3. Scope

2.3.1. This policy applies to all information, information systems, networks, applications, locations and users of Truro & Penwith Academy Trust or supplied under contract to it. This includes hardware such as laptops and mobile devices.

2.4. Risks

2.4.1. On occasion, Truro & Penwith Academy Trust's information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance, may intentionally or accidentally gain unauthorised access to Truro & Penwith Academy Trust]'s information which may adversely affect day to day business. This policy is intended to mitigate that risk.

2.4.2. Non-compliance with this policy could have a significant effect on the efficient operation of Truro & Penwith Academy Trust and may result in financial and/or reputational loss and an inability to provide necessary services to our schools and learners.

3. Physical Access

3.1. Physical Access is every individual's responsibility for any device they are issued or use to access Truro & Penwith Academy Trust's systems.

3.2. Individuals are to:

3.2.1. Ensure that the location of device(s) issued to them are known at all times.

3.2.2. Ensure they follow the mandatory password access controls for devices in Truro & Penwith Academy Trust's.

3.2.3. Prevent access to any Truro & Penwith Academy Trust device or device accessing Truro & Penwith Academy Trust's data from any person not authorised by Truro & Penwith Academy Trust to access the device and data.

3.2.4. When they are not using the device they must ensure that the device is locked and any display screen or any other access port available via the device must be made secure from unauthorised viewing or access prior to leaving the device.

3.2.5. Devices may not be left unattended in the office at any time when there is no Truro & Penwith Academy Trust employee present.

3.2.6. Devices that are to be left in the office for an extended period of time or overnight must be shut down to enforce password protection.

3.2.7. Access to physical network devices within the Truro & Penwith Academy Trust offices is restricted.

3.2.8. Access to the network room is controlled by Jamie Pilcher who maintains a register of personnel permitted to access and operates a controlled key process to maintain security.

3.2.9. Any suspected or known unauthorised access to a device must be reported immediately to the Data Protection Officer, Josie Medforth dpo@panoramic.org.

4. Physical Access Buildings

4.1. Physical Access to the Truro & Penwith Academy Trust's office is controlled by alarm and key Reception is administered by Emily Burley and other administration support.

4.2. Only Truro & Penwith Academy Trust employees will be permitted to apply for a building security or personal ID access pass.

4.3. Access to Truro & Penwith Academy Trust is manned by personnel between 9am and 5pm

4.4. All people entering the building are required to use their issued pass to gain access.
4.5. Where an individual does not have a pass or their pass is not authorised or expired, reception/security will prevent further access to the building.
4.6. All guests must be notified to the reception and security to have access to the building and are not permitted to pass the reception area without being escorted by a member of staff.
4.7. On termination of employment immediately to terminate pass credentials.
4.8. Any key issued must be returned to Judy Brinson on termination of employment.
4.9. Cleaning staff are permitted access to Truro & Penwith Academy Trust for cleaning only and are instructed to notify Judy Brinson of any device found unsecured during their cleaning.

5. Passwords

5.1. Choosing Passwords

5.1.1. Passwords are the first line of defence for our IT systems and together with the user ID helps to establish that people are who they claim to be.

5.1.2. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our information, computers and systems.

5.2. Defining 'weak' and 'strong' passwords

5.2.1. A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

5.2.2. A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

5.2.3. Everyone must use strong passwords with a minimum standard of:

● At least ten characters.

● Contain a mix of alpha and numeric, with at least one digit.

● Is not based on anything, which could be guessed easily by someone or obtained from personal information such as name, telephone number or date of birth.

5.3. Storing Passwords

5.3.1. The best way to store passwords is by using a password manager. This provides a central repository for passwords and promotes good credential management, especially the creation of complex and unique passwords.

5.4. Protecting Passwords

5.4.1. It is of utmost importance that passwords remain protected at all times. The following guidelines must be adhered to at all times:

● Never reveal your passwords to anyone.

● Never write your passwords down or store them where they are open to theft. ● Never store your passwords in a computer system without encryption.

● Do not use any part of your username within the password.

● Do not use the same password to access different systems.

● Do not use the same password for systems inside and outside of work.

5.5. Changing Passwords

5.5.1. Default passwords must be changed immediately.

5.5.2. If you become aware or suspect that your password has become known to someone else, you must change it immediately and report your concern the Data Protection Officer, Josie Medforth dpo@panoramic.org

6. Team Member Access

6.1. User Access Management

6.1.1. Each user must be allocated access rights and permissions to computer systems and data that;

● Are commensurate with the tasks they are expected to perform.

● Have a unique login that is not shared with or disclosed to any other user.

● Have an associated unique password that is requested at each new login.

7. User Registration

7.1. Access to Truro & Penwith Academy Trust's information services is controlled.
7.2. Each user is identified by a unique user ID which will take the form of their individual company email address.

7.3. This unique ID will be used to grant access to any system or software so that users can be linked to and made responsible for their actions.

7.4. There is a standard level of access (email access, file access, authorised software, printing and document scanning), other services can be accessed when specifically authorised.

7.5. Access to all Truro & Penwith Academy Trust systems is provided by TPAT IT Support

7.6. When a team member leaves Truro & Penwith Academy Trust their access to computer systems and data must be suspended at the close of business on the team members' last working day. It is the responsibility of the team members' team leader to request the suspension of the access rights to the TPAT IT Support

8. User Responsibility

8.1. It is a user's responsibility to prevent their user ID and password from being used to gain unauthorised access to Truro & Penwith Academy Trust's systems by;

- Following the Password Policy Statements outlined above.
- Ensuring that any Laptop or PC or other device, when left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing a member of the IS Team if their role and access requirements change at any time.

9. Remote Working

9.1. Any mobile devices including laptops, tablets and phones that have access to Truro & Penwith Academy Trust emails or data must use a VPN service when using a public WiFi connection. TPAT uses SoftEther as a mandatory VPN.

10. Network Access Control

10.1. The use of non-authorised modems/routers/networking devices connected to Truro & Penwith Academy Trust's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from [insert the name or appointment] before connecting any network equipment to Truro & Penwith Academy Trust's network.

10.2. User Authentication for External Connections

10.2.1. Where remote access to Truro & Penwith Academy Trust's network is required, an application must be made via the TPAT IT Support Manager. Remote access to the network must be secured either by a supplied VPN or two-factor authentication consisting of a username, password and one other component, for example, an OTP sent to a mobile phone.

10.3. Operating System Access Control

10.3.1. Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the password section must be applied. The login procedure, where possible, should also be protected by;

- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.

10.3.2. All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights). System administrators must have individual administrator accounts that will be logged and audited.

10.4. Application and Information Access

10.4.1. Access within software applications must be restricted using the security features built into the individual product. The access must;

- Be compliant with the User Access Management section and the Password section.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

10.5. Software Installation

10.5.1. Truro & Penwith Academy Trust controls and restricts the use of all utility programs (such as anti-virus, disk cleaner, file managers, screensavers, etc.) and other software programs by maintaining a compiled list of approved software.

10.5.2. This list is available for all team members to view.

10.5.3. Truro & Penwith Academy Trust's procedure for authorising untested software is performed by TPAT IT Support. Team members must contact IT Support directly, and an assessment will be carried out to determine if the desired software is suitable for Truro & Penwith Academy Trust.

10.5.4. If confirmed, the software is added to the approved software list.

10.6. Applying the Policy - Privilege Management

10.6.1. "Special privileges" are those allowed to the system manager or system's programmers, allowing access to sensitive areas (for example, passwords, customer or company data). The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached.

10.6.2. Privileged access must be requested and authorised by Data Protection Officer, Josie Medforth dpo@panoramic.org .

11. Further Information

11.1. Further information and advice on this policy can be obtained from the manager of TPAT IT Services.

Signed via Google Form. This is to say that you have read and understood this policy. It is timestamped and can be referred to by the Headteacher for future reference