Trust in Learning
Trust in Success

TRUST IN LEARNING (ACADEMIES)

INFORMATION SECURITY POLICY

Trust in Learning
Trust in Success

Trust in Learning
Trust in Success

Date Created: April 2018
Effective From: April 2018
Dated Adopted by the Board: May 2018
Review Date: September 2023

Date	Page	Change	Purpose of Change
May 2018		New Policy	
October 2019		Various changes to policy	
September 2022		No changes	

1. Introduction

1.1 Information is one of the Trust's most important assets. Failure to ensure adequate security and protection of information held by the Trust and its associated schools may lead to legal action against the Trust and/or the individual responsible for the breach. Such legal action could include an investigation by the Information Commissioner's Office ("ICO") who can impose significant financial penalties and/or a claim for damages for breach of the General Data Protection Regulation and the Data Protection Act 2018 (together the "Data Protection Legislation").

1.2 In addition to the possibility of legal action being taken against the Trust, if the information held by the Trust and its associated schools is not kept safe, confidence in the Trust and its associated schools by pupils, parents, guardians, volunteers, the Board of Governors, members of staff and the public at large could be irreparably damaged.

1.3 Keeping information secure yet available to those that need it often presents a difficult challenge. This policy strives to achieve a sensible balance of securing the information held by the Trust while making it accessible to those who need the information. The Trust will always however favour security over accessibility where there is any doubt as to the security of information.

2. Definitions

2.1 *The Trust"* means Trust in Learning (Academies) and its associated schools.

2.2 *"Data Protection Legislation"* means the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2.3 *"Data"* means Personal Data and Special Category Personal Data as defined by the *Data Protection Legislation*, and confidential and sensitive information held by the Trust.

2.4 *"Personal Data"* and information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.5 *"Special Category Personal Data"* means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

2.6 *"Processing"* means any activity that involves use of data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

2.7 *"Data Controller"* is the organisation which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. The Data Controller referred to in this policy is Trust in Learning (Academies).

2.8 *"Data Protection Officer"* is the person within the organisation who is responsible for overseeing data protection strategy and implementation to ensure compliance with data protection legislation.

2.9 "*Data Subject*" means all living individuals about whom the Trust holds Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in respect of their Data and the information that the Trust holds about them.

2.10 *"Data Processor*" means any person who or organisation which processes Data on behalf of the Data Controller including members of staff, volunteers, contractors, and suppliers and any third party whose work involves accessing or otherwise using Data held by the Trust. Data Processors have a duty to protect the information they process for and on behalf of the Trust by following this and other Trust information governance policies at all times.

2.11 *"Subject Access Request* ("SAR") means a request by an individual to the Trust pursuant to Article 15 of the GDPR.

2.12 *"Information Asset"* means Data held by the Trust in any form. This Data may be held electronically by software in computer systems and transferred across a network, on paper, in files or transferred by post, courier or in person.

2.13 "*Information Governance Policy*" means the Data Protection, Freedom of Information, Information Security, Retention, Disposal and Records Management and Subject Access Request policies and any other policies which may from time to time be in place at the Trust.

2.14 "*ICO*" means the Information Commissioner's Office.

2.15 "*Information Security*" means the protection of information and information systems against unauthorised access to or modification of information, whether in electronic or manual storage, Processing, transit and against the denial of service to authorised users.

2.16 "*Information Security Breach*" means a breach which may be caused by a technical failure, unauthorised access to either the Trust's networks or a Client Device used for Trust business by a third party, loss of the Trust's information and/or inappropriate actions of an individual or individuals which result in the compromise of information belonging to or held by the Trust.

2.17 "*Information Security Vulnerability*" means an identified weakness of a system(s) or process that puts the security and availability of information at risk.

2.18 "*Member of Staff"* means individuals working at the Trust whether on a full time, part time, temporary, fixed term, casual or volunteer basis.

2.19 *"Client Device*" means the use of laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment that could be used for the carrying out of Trust business or the Processing or storing of information.

2.20 *"Personal Device"* means a Client Device not directly owned by the Trust.

2.21*"Username" means a unique sequence of characters used to identify a person, system or service, allowing access to a computer system, computer network, client device, or online account.*

2.22*"Strong Password" means a phrase of sufficient random characters to prevent guessing or brute-force attacks. A Strong Password must be a minimum of eight characters, does not use single common number sequences/dictionary words or easily accessible personal information (ie any portion of your name, date of birth, telephone numbers or NI numbers).*

2.23*"Secure Authentication Device"* means a device or component integrated into a Client Device that allows the encrypted storage and retrieval of Strong Passwords using biometric information.

2.24*"Two-Factor Authentication (also known as Multi-Factor Authentication, MFA or 2FA)"* means a method of confirming a claimed identity using a combination of at least two of the following categories: knowledge (something they know, eg a password), possession (something they have, eg a token), and inherence (something they are, eg a fingerprint).

2.25*"Authorised User"* means a person, or administrative service, that is authorised by the Trust to authenticate to a system, that may contain Data and potentially to receive authorisation to access resources provided by or connected to that system.

2.26*"Removable Media"* includes USB sticks, external hard drives, CD's or other media which can be connected to the Trust's network or a Client Device and used for storing information.

2.27*"External"* means any and all buildings, systems or services not directly owned by the Trust.

2.28"*Social Media"* means websites and applications that enable users to create and share content or to participate in social networking including Facebook, LinkedIn, Twitter, Google+, and all other social networking sites, internet postings and blogs. It applies to the use of Social Media for Trust purposes as well as personal use that may affect the Trust in any way.

2.29 "*Cloud service*" Cloud computing/Service is the delivery of computing resources using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local servers or a personal computer.

3. Summary

3.1Much of the information held by the Trust is confidential and sensitive in nature. Therefore it is necessary for all information systems to have appropriate protection against adverse events (accidental or malicious) which may put at risk the activities of the Trust or protection of the information held.

3.2The Trust has a responsibility to maintain:

i. **Confidentiality** – access to Data must be confined to those with specific authority to view the Data in question;

ii. **Integrity** – information should be complete and accurate. All systems, assets and applicable networks must operate correctly and according to any designated specification;

iii. **Availability** – information must be available and delivered to the right person at the time when it is needed and in accordance with the relevant statutory provisions.

3.3 The Trust must minimise the risk of data security breaches and any person connected to or acting on behalf of the Trust must meet the minimum requirements as set by the Trust for connecting to any

network operated by or on behalf of the Trust. This can be found in Appendix 2

3.4 It is important that members of staff, governors or anyone else acting on behalf or with the authority of the Trust:

i. Are aware of how and under what circumstances they are permitted to access Personal Data held by or on behalf of the Trust.
ii. Is aware of who they are allowed to share Personal Data and other information with and how it can and should be shared.
iii. Reports any Information Security incidents/breaches including phishing emails[1] to the Data Protection Officer in respect of information held by the Trust. Staff and governors must follow the Data Breach flowchart in Appendix 3
iv. Ensures Data is stored and handled securely and in accordance with this and the other information governance and IT Policies.
v. Does not ignore, turn off or otherwise bypass any Information Security controls put in place by the Trust.
vi. Does not send, distribute or otherwise divulge Data unless permitted to do so. The sending or distribution of any Data should only be done in accordance with the applicable statutory provisions, this policy and any other applicable policy of the Trust.
vii. Data must only be sent by secure methods and, all Data sent externally shall be encrypted.

4. Policy Statement

4.1 It is essential that the Trust's information systems and data networks are adequately protected from events which may compromise the information held or the carrying on of Trust business and to this end the Trust is committed to developing and maintaining an information systems structure which has an appropriate level of security.

4.2 The Trust will maintain the security and confidentiality of Data held by it, its information security systems and relevant applications and networks for which it is directly responsible by:

i. Ensuring appropriate technical and organisational measures are in place to prevent unauthorised access, damage or interference to and/or with information, IT assets and network services;

ii. Ensuring that it is aware of, and complies with, the relevant legislation as described in this and the other information governance and IT Policies;

iii. Describing the principles of Information Security to Members of Staff, pupils, governors and volunteers and explaining how they will be implemented by the Trust;

iv. Creating and maintaining a level of awareness of the need for information security to be an integral part of the conducting of Trust business and ensuring that everyone understands their individual and collective responsibilities in this respect;

v. Protecting Data and other information held by and/or on behalf of the Trust.

4.3 To ensure a consistent approach to Information Security, the controls set out at paragraphs 7 and 8 of this policy will apply.

5. Use of Client and Personal Devices

[1] An email sent in an attempt to acquire sensitive information such as usernames, passwords or financial information.

5.1 Client Devices used for, or in connection with, Trust business and in particular for the collection or storing of Personal Data and/or Special Category Personal Data must be kept secure with Strong Passwords (see Definitions). If available with the device, an approved Secure Authentication Device to aid entering the password

5.2 Client Devices used for, or in connection with, Trust business must not be left unattended in plain sight at any time, including whilst at home or travelling, and must be protected against loss, damage, misuse or unauthorised access. When not in use, Personal Devices must be stored in a secure lockable location and should never be stored in vehicles, even if locked

5.3 Client Devices used for, or in connection with, Trust business must not be used to access, view or process Personal Data or Special Category Personal Data in a manner that allows Persons other than the Authorised User to view the Data

5.4 Personal Devices, including but not limited to, laptops, tablets, telephones, smartphones, desktop computers or other electronic equipment, must not be used to store or transmit Data. Where a Member of Staff believes there is a legitimate need to process Special Category Personal Data using a Client Device, the Member of Staff should contact their Line Manager with a business case for the provision of a Client Device, who shall evaluate the business case for such request

5.5 Client Devices used for, or in connection with, Trust business must be updated with the manufacturer's software and other updates regularly when updates become available, and where supported have antivirus software installed and regularly updated

5.6 Client Devices used to store Personal Data or Special Category Personal Data must be encrypted

5.7 Client Devices issued to a Member of Staff for or in connection with, Trust business by the Trust must only be used by Trust Members of Staff. At no time shall any other User, including but not limited to, family members, friends, employee from another organisation, be permitted to use the device

5.8 If a Client Device used for, or in connection with Trust business is lost or stolen, the loss/theft should be reported to the Data Protection Officer and the IT Support Team as soon as possible and in any event within 24 hours of the loss/theft occurring. Where possible the Client Device should be remotely accessed and the information erased

5.9 Before using a Personal Device for, or in connection with Trust business, users must read and sign the Personal Devices Statement found in Appendix 1

6. Removable Media

6.1 Removable Media must only be used as a last resort, when all other options have been considered

6.2 Only Removable Media provided by the Trust that has been encrypted should be used for the storing of Data

6.3 Removable Media should not be used for the storing of Personal Data, Special Category or Sensitive Data

6.4 Removable Media must be stored securely

6.5 If Removable Media used for, or in connection with Trust business is lost or stolen, the loss/theft should be reported to the Data Protection Officer and the IT Support Team immediately

7. Securing Information

7.1 **Physical Access Controls**

i. A nominated member of the Trust will be responsible for ensuring the Information Security of all Information Assets held by or on behalf of the Trust. The nominated person will also have and maintain an Information register which should record all Information Assets held by the Trust;

ii. A copy of the Information register will be filed with the Director of Finance and Operations at the Trust each year.

iii. The Trust will ensure that only authorised individuals are allowed access to restricted areas containing Personal Data or Special Category Personal Data or information systems where there is an identifiable need to access that area;

iv. Access to Personal Data and/or restricted physical locations will be monitored by the Trust's nominated person to ensure authorised access to relevant information and to prevent unauthorised access to Personal Data or Special Category Personal Data;

v. Where an unidentified person or any other person without authorisation to be in a restricted area is found, the individual is to be challenged as to their identity and the purpose for which they are in the restricted area. If the unauthorised individual has no legitimate reason to be in the restricted area, this information is to be logged as an Information Security Breach and the Data Protection Officer should be consulted as to whether the matter requires reporting to the ICO;

vi. External doors and windows must be locked at the end of each day.

vii. Equipment that serves multiple users must be capable of identifying and verifying the identity of each authorised user when equipment is connected to the domain.

viii. Devices or equipment capable of displaying output upon multi-user displays or presentation equipment, including but not limited to, Projectors, Interactive Whiteboards, televisions, video walls, remote computer sessions and desktops, or any other form of presentation equipment, must not be used to access, view or process Data in a manner that allows Persons other than the Authorised User to view the Data

ix. Members of staff of the Trust with access to and use of Data must maintain a clear desk and clear screen policy to reduce the risk of unauthorised access to Information Assets such as papers, media and information processing facilities.

x. Personal Devices and computers whether belonging to the Trust that are used for, or in connection with Trust business must be switched off or controlled by a complex password (see definitions) when unattended or not in use.

xi. Data recorded on paper must be kept locked away in a safe, cabinet or other form of secure furniture when not in use.

xii. Personal Data and Special Category Personal Data, confidential and sensitive information about the Trust whether stored electronically or on paper must be kept locked away in a secure room or in a safe, cabinet or other form of secure furniture when not in use.

xiii. Documents containing Data must not be left unattended at mail points or on printers, photocopiers, scanners or fax machines and must be removed immediately when received.

7.2 **Password and Access Control**

i. Access to Data stored electronically must be controlled through the use of a Strong Password

ii. Access to Authorised User accounts must be controlled, as a minimum through the use of a password, which must not be less than eight ASCII characters in length. Wherein, a system or service, provides alternative authentication methods, including but not limited to, facial or biometric recognition, the alternative authentication method must be in addition to a password

iii. Members of staff must ensure that they have a Strong Password for all Authorised User accounts and the same password not re-used across different types of system

iv. All Authorised Users, aged 11 or over after the 1st September each year, should ensure they have a Strong Password for all accounts

v. Authorised Users are responsible for keeping their assigned password(s) secure and must ensure their password(s) is neither disclosed to, nor used by, anyone else under any circumstances

vi. User of another person's username or password will constitute an Information Security Breach and must be reported in accordance with the procedures set out in this policy or any other relevant policy from time to time in force

vii. Authorised Users are responsible for ensuring that all Trust and/or Client Devices used to access Data or other confidential information, are logged off, switched off or otherwise controlled by a Strong Password when unattended or not in use, at all times

viii. Authorised Users with access to the Trust network or a Client Device which is used for, or in connection with Trust business is responsible for any actions carried out under their username and password

ix. Where available, Members of Staff using critical systems or accessing Personal or Special Category Personal Data should use Two-Factor Authentication.

7.3 **Cloud Computing**

i. Only cloud computing networks or services, including Social Media commissioned by the Trust, or expressly authorised by the Data Protection Officer, may be used to store and send information concerning or relating to Trust business. The use of personal cloud storage solutions (Skydrive, Onedrive, Personal, iCloud, G-Drive etc) for the transfer of Trust information is expressly forbidden

ii. Personal Data, Special Category Personal, confidential and sensitive information, whether on the Trust network or a Client Device must not be stored on a cloud computing network or service not commissioned by the Trust, or expressly authorised by the Data Protection Officer

iii. If Data or other information concerning or relating to Trust business is to be stored in or on a cloud network, the Trust will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any Data transferred outside of the EEA

iv. If the Trust receives notification that Data in respect of Trust business has been corrupted, lost or otherwise compromised while stored on a cloud network, the Trust should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information

v. Any corruption, loss or compromise of information held on a cloud network should be recorded in the risk register and if appropriate reported via the mandatory reporting procedure as set out at Section 9 of this policy

8. Leaving the Trust/Contract Termination

i. Upon leaving the Trust, Members of Staff must return/transfer, in a useable format, all equipment and information, including Data to the Trust, on or before the agreed leaving date (ie last day of employment) to their Line Manager, or other Trust representative if their Line Manager is not available. This includes, but is not limited to:

- All information, including data, used or stored as part of the role, both physical and electronic
- All information, including files, documents and emails, including any Data, stored within individual Cloud Service accounts
- Client Devices loaned by the Trust, including PIN numbers, usernames or passwords required to reuse or reset the devices
- Any Removable Devices provided by the Trust
- Access control, PIN, tokens and ID cards
- Keys and PIN numbers used to access physical locations

ii. After leaving, Members of Staff may not attempt to access or use any Trust information, including any Data

9. Storing and Transportation of Non- Electronic Data

9.1Data can be vulnerable to loss, unauthorised access, misuse or corruption when being physically transported either personally by Members of Staff of the Trust or when sending Data via the postal service or couriers;

9.2Special controls should be adopted to protect Data from unauthorised disclosure or modification and include:

i. Ensuring the packaging if sufficient to protect the contents from any physical damage likely to arise in transit
ii. Delivering by hand records containing Personal Data, where appropriate
iii. Sending Data via secure post such as Royal Mail recorded or signed for delivery or special delivery or as otherwise agreed with the Data Subject;
iv. Records containing Special Category Personal Data shall not be delivered by hand unless absolutely necessary. In which case the following should occur:
    a. Documents transported in vehicles should be hidden away or placed in boot where possible, and the vehicle locked
    b. Documents should never be left unattended even in a locked vehicle.

9.3 Consideration should be given to the necessity of transporting or moving Data or other records as this increases the risk of Data loss.

10. Transportation/Transmission of Electronic Data

10.1 Personal Data, Special Category Personal, confidential and sensitive information sent or transmitted externally using an electronic systems or services must be secured using a process that ensures the Data is encrypted and Users must carefully check the recipient's contact details before sending

10.2 Data must only be sent or transmitted externally when authorised by job description, Trust policy, applicable legislation, or when specially authorised by the Data Protection Officer. The sending of Personal Data and Special Category Personal Data to personal cloud systems or services email accounts is expressly forbidden. Members of staff working remotely are required to access Data through the Trust's authorised systems and services

10.3 Data must not be sent using any systems or services, including but not limited to, cloud platforms and social media providers or any other type of system not approved for use by the Trust, including text messaging

10.4 Personal Data and Special Category Personal Data must be sent to named Users only. Multi-User posting, send or transmission, including, but not limited to, email lists, distribution groups, security groups, chat/team-based groups, forums, rooms, and channels is prohibited.

11. Information Security Incident Reporting and Management

11.1The Trust will have and maintain a register where all Information Security incidents are logged. This log as a minimum should include:

i. The nature of the breach;
ii. The number of Information Assets compromised;
iii. How the Information Asset(s) has/have been compromised;
iv. Whether any Special Category Personal Data was compromised;
v. Whether the incident needs to be reported in accordance with the mandatory reporting section of this policy at paragraph 11.3 below.

11.2 Where there has been any breach the Data Protection Lead must be informed immediately, so they can decide if an Information Security Breach has occurred and if the DPO should be involved in order that consideration can be given to reporting the breach to the appropriate authorities;

11.3If there has been an Information Security Breach but it does not require reporting to the ICO, it should be recorded in the Schools Information Security Incident Log;

11.4Examples of an Information Security Breach include but are not limited to:

i. Password(s) written down or stored, in an accessible, plain text or otherwise visible, manner to persons other than the Authorised User;
ii. Using another person's password;
iii. Divulging of a password;
iv. Making use of Personal Data for personal gain;
v. Accessing Data for personal knowledge;
vi. Attempting to gain access under false pretences;
vii. Unauthorised release of Data;
viii. Knowingly entering inaccurate Data;
ix. Deleting Data prior to the retention period or any other period set out in the Retention, Disposal and Records Management policy expiring;
x. Loss or misuse of Data;
xi. Malicious damage to equipment or Data;
xii. Changing permissions that allows access to, or sharing information (including Data) with, persons not authorised to access the information
xiii. Unauthorised removal of Data, Trust equipment or equipment used for or in connection with Trust business from Trust premises or another site authorised for the storage of such information or equipment
xiv. Loss or theft of a Client Device used for or in connection with Trust and/or Trust purposes or any other device belonging to the Trust or Trust.

12. Business Continuity and Disaster Recovery Plans

12.1Each school will develop a managed process to counteract the interruption of Trust business caused by major IT service failure. The Trust will ensure that business continuity and disaster recovery plans are produced for all IT systems and networks which store and/or Process Data.

12.2 The Trust will have procedures in place to maintain essential services in the event of an IT system failure.

13. Monitoring and Review

11.1 This policy will be reviewed every four years or earlier if required and may be subject to change.

APPENDIX 1

Personal Devices Statement

Trust in Learning (Academies) recognises that its employees will use personal devices to access work information and emails. This must be achieved with appropriate protection of the data that is held within the documents. Therefore all Employees using personal devices to access Trust documents and emails must adhere to the below requirements.

Personal devices include but not limited to mobile phones, tablets, laptops and PCs.

Personal Devices used for, or in connection with, Trust business must be encrypted and should be kept secure at all times and be protected against loss, damage, misuse or unauthorised access. When not in use, Personal Devices must be stored in a secure location, and should never be stored in vehicles, even if locked.

Personal Devices are expressly prohibited from being used to store or externally transmit Special Category personal Data at any time.

The use of Personal Devices for, or in connection with, other Trust business should be kept to a minimum to reduce the risk of unauthorised access to, or disclosure of, information held by the Trust, and must be updated with the manufacturer's software and other updates regularly when updates become available, and where supported have antivirus software installed and regularly updated.

Subject to the requirement of a Strong Password (see below) for access, if the Employee is the only person with access to the personal device that is being used for Trust work, then documents, apps (including email) and web-based programmes may be left open on the device, whilst the device is locked or logged out.

If a personal device is not solely used by the Employee, then if supported, the device must be configured with separate user accounts for each user, so that the Employee has their own device logon account and others cannot access any documents, apps (including email) and web-based programmes they have open. If the device does not support separate user accounts, or the device is accessible to other people (such as family members, other employees), any documents, apps and web-based programmes must be closed when not in use, and require a password to access the data when re-opened.

Passwords

All Trust data, in particular Personal Data and/or Special Category Personal Data must be kept secure with Strong Password at all times

When not in use the user account or personal device must require a Strong Password to 'login', 'unlock' or access any information or Data using the device.

Definition of a Strong Password is available in the Trust's Information Security Policy.

Lost or Stolen Personal Devices

If a personal device is lost or stolen and has access to Trust information on it, the following actions must be taken.

1) Contact the School Business Manager (Data Protection Lead) immediately, who will assess the risk of loss of data.

2) Immediately remotely access the programme (i.e emails) and change the password or

3) Contact the Trust's IT support team immediately. They will be able to remotely reset passwords for services provided by the Trust.

APPENDIX 2

Minimum security standards for networked client devices

Trust in Learning (Academies) Information Security Policy requires all network capable devices that connect to any Trust network(s), comply with the following minimum security requirements.

The requirements help to protect both the individual client device and other client devices connected to the Trust's network(s).

In the event that a client device cannot demonstrate that it meets the minimum requirements, the device must not be connected to the network, unless written authorisation is provided by the CEO/Headteacher or Authorised Personnel.

Software Patch Updates

Client devices must only use operating systems and software applications that are supported by the manufacturer. The client device must be able to demonstrate that all currently available security patches have been installed, and that there is a recurring schedule to notify the user of future updates.

Anti-virus/malware Software

Client devices must be configured to use and run, anti-virus/malware software that utilises real-time scanning and/or scans the entire device at least once a day. The anti-virus/malware software must also be configured to receive software and virus/malware definition updates regularly.

Authentication

Client devices must not provide unauthenticated user access. User authentication must be provided by means of strong passphrases or other secure authentication mechanisms.

Unnecessary Software or Services

Devices must not run any software applications or services for any purposes, other than the agreed intended use.

No Unattended User Sessions

Users must not leave the device unattended when logged in or with an active session open. The user must manually suspend or close the active session when they are not using the device. Due to the nature of teaching and learning, Trust devices/operating systems should be configured to automatically lock after 1 hour of inactivity, to allow reasonable instruction time.

Firewall Software

Client devices should be configured to use an active client-based firewall. The firewall software should be configured to only allow incoming traffic for the intended use.

Privileged User Accounts

Client devices should support the separation of user account privileges, to reduce the risk of malware spreading across the network. All users should be aware that a standard account should be used for non-administration tasks at all times.