JOHN TAYLOR MULTI ACADEMY TRUST

ICT Security - Encryption

Policy Owner:	**Mark Crompton, JTMAT Strategic Network Manager**
Implementation date:	September 2016
Reviewed on:	November 2022
Next review date:	November 2023

Table of contents

Version Control

Version	Author	Date	Changes
1.0	M. Crompton	21/04/2017	First Draft
1.1	M. Crompton	26/10/2017	Amendments as per the Audit Committee (RE: Email dated 12th October 2017)
1.2	M. Crompton	22/11/2017	Amendments as per the Audit Committee (RE: Email dated 12th October 2017)
1.3	M. Crompton	12/11/2021	Review and updates RE: Multi Factor Authentication
1.4	M. Crompton	08/11/2022	Amendments to reflect practice including the introduction of MFA, remote access and student accessible area.

Context

The protection of electronic information and access to removable storage is vitally important – especially with the increasing demand to use ICT systems to perform data analysis across the Trust. Protecting a person's identifiable information and Trust's information (e.g. Examination Results, photographs or contact lists) from unauthorised access, disclosure or loss whether it be by theft or accident is of paramount importance.

Encryption provides a level of protection for the storage, retrieval and access to data. Encryption works by converting data to make it inaccessible and unreadable to unauthorised individuals. The only way to read encrypted data is by using a decryption key. Common decryption keys can be passwords, Smartcards or USB storage keys.

The Data Protection Act, specifically Principle 7 requires the Trust to have appropriate policies and procedures in place to ensure the safe keeping, use, retrieval and access to data. The Trust as a Data Processor/Controller has an additional responsibility to ensure the integrity, security and protection of all data which it holds**.**

Purpose

The purpose of this policy is to:

- Detail the specification and deployment of data encryption software
- Provide guidance on the use and handling of portable media
- Describe how encryption will be used and applied to devices
- Detail a method for;
    - reporting breaches of this policy
    - reporting the theft or loss of data

Scope

This policy covers all electronic data and details the types of devices which are acceptable for the storage and the transmitting of data, and how these devices utilise encryption software irrespective of whether or not the data held on them is considered confidential or sensitive. The policy and procedure applies to all users, regardless of length of service, but does not form part of the contract of employment and can be varied from time to time and in consultation with the appropriate bodies. The Trust reserves the right to take action against individuals who breach this policy regardless of current employment status within the Trust.

The policy covers encryption for the following devices and applications;

- Desktops and laptops
- Handheld devices such as mobile phones, PDAs or tablets
- Portable/removable storage e.g. USB memory sticks and external drives
- Removable media e.g. DVDs/CDs and backup tapes

- Remote Access
- Shared Areas
- Email

More information can be found regarding general security of information and acceptable use of Trust owned resources by consulting the relevant policies or by contacting JTMAT IT Services.

Encryption Technology

The school has adopted Microsoft BitLocker in order to provide a robust solution for protecting and encrypting data.

Microsoft BitLocker uses the AES 256-bit (Advanced Encryption Standard) which is a symmetric-key encryption with a 256-bit key. In addition BitLocker also uses a Diffuser algorithm to help protect against ciphertext manipulation attacks which attempt to find weaknesses and patterns when encrypted data is changed. To find out more about the encryption technology used by BitLocker visit the Microsoft Webs Site: How Strong Do You Want the BitLocker Protection?

Responsibilities

Trust & Individual Schools/Academies

The Trust is responsible for the implementation of this policy. Each individual academy has a responsibly to provide its employees with an appropriate method, procedures and software to secure all electronic data. The use of portable devices may be subject to random periodic review by the Trust to ensure compliance with this and other Trust policies.

Staff – Permanent or Supply

All Trust employees have a duty to abide by this policy to ensure the safe and secure handling, transmitting and retrieval of all electronic data **at all times**. On termination of your employment all removable media containing sensitive or confidential data should be removed along with any encryption.

Students

Students are not expected nor will they be forced to encrypt removable devices or files as typically they only have access to limited information about themselves or others. It is also presumed they receive adequate information and guidance during ICT lessons on the value of protecting their own data. If evidence of this is required please contact the appropriate IT coordinator to obtain a Scheme of Work.

Third Parties (Contractors, agencies & consultants)

If any other person (not named above) is granted access to the Trust's computer system they will have the same responsibilities as defined in the "Staff – Permanent or Supply" section above.

Upon termination of their contract any personal, sensitive or confidential information held must be deleted.

General Rules

Trust employees who are issued with portable storage devices including laptops or tablets, are able to write to portable storage media or view / transmit data have a responsibility to ensure:

- No one other than authorised person/s are aware of the encryption/decryption password for the device, media or system.
- Any portable device or media is not given to any unauthorised persons for safe keeping.

- Any portable device or media is not left discarded or unattended in a public place.
- When using remote access do not use public/free Wi-Fi.
- All reasonable steps are taken to ensure that during transit, any portable device/media are securely stored. Portable devices/media must not be left unattended in any vehicle at any time due to RPA insurance requirements.
- Any portable device or media is adequately protected from physical damage.
- Any portable device or media is not hired, lent out or given without authorisation from IT Services.
- Any portable device or media which is no longer required or has reached its lifespan must be handed in to IT Services. All data on the device / media must be wiped, destroyed and disposed of.
- The device / media is handed back to the IT Services on cessation of employment with the Trust.
- The loss of any portable device is immediately reported to IT Services.

Devices and Applications

Due to the complex nature of encryption and the many forms in which information can be transmitted there are different rules depending on the device and/or application being used. The section below covers the major forms in which information can be accessed or transmitted but is in no way exhaustive;

Desktops and Laptops

Full disk encryption will take place on these devices utilising BitLocker or other appropriate software/hardware.

Handheld Devices

All handheld devices are to be encrypted to ensure data is secure if stored locally, this process is elective and is the responsibility of the device owner. If you require assistance please contact IT Services who will guide you through the process.

If a handheld device (personal or school owned) is to be used to access Trust systems the user will be required to:

- Encryption is enabled on the device
- Encryption is enabled on the storage card
- Setup appropriate security measures e.g. password, biometric or passcodes
- Ensure Multi-factor Authentication for Trust systems is configured

Portable USB Sticks or drives

On insertion of any (personal or Trust owned) USB storage device the user will be prompted to encrypt the device and set a password. Encryption can only take place on a domain joined machine that has a live connection to the network; this is required to store the recovery key. The password will need to conform to the Trust's Password Policy. If you fail to encrypt a device it will be in a read-only state.

Encryption on large drives can take a considerable amount of time, it is requested any large drive over 200Gb be encrypted by IT Services.

Removable Media (DVDs/CDs)

Where there is a need to move sensitive or confidential data using removable media such as DVDs/CDs or backup tapes these will need to be encrypted using the following method:

1. Burn or copy the encrypted file to the media
2. Send the media to the required person; never send the password with the media
3. Then either;
    a. Phone the recipient, confirm their identify, then disclose the password
    b. Email the password separately

Remote Access (Remote Desktop)

Remote access is secured using two different security certificates both encrypting data to the AES 256-bit standard and validating the computers you are connecting to. In order to prevent data loss by accessing this service from an external computer the following security settings have been applied:

- Access to the system is granted to JTMAT employees
- Access to the local file system has been prevented in order to stop unencrypted files being transmitted and stored
- COM port mapping has been prevented
- Clipboard is disabled to prevent information being copied from/to your local device
- Printing is disabled to prevent unauthorised copies of documents being printed
- An idle timeout is set at 1 hour, after this time you will automatically be disconnected
- A maximum session time of 8 hours is allowed before you are forced to reconnect

Email

When sending any personal, sensitive or confidential data via email the following best practice should be adopted:

1. **DO NOT SEND EMAIL** containing personal, sensitive or confidential information to your personal email address or email addresses such as:
    a. user@gmail.com
    b. user@googlemail.com
    c. user@yahoo.com
    d. user@hotmail.com
    e. user@outlook.com
2. Only send email to a person's organisational email such as:
    a. user@staffordshire.gov.uk
    b. user@nhs.co.uk
    c. user@dfe.gov.uk
3. Ensure you know the recipient and have their correct details, confirm with them if necessary. If you are unsure if the person should be receiving the information contact your Data Protection Lead who will be able to advise you as necessary.
4. Attach and send the encrypted files to the person ensuring the word "Confidential" appears in the subject line or use the built in encryption tools in Outlook (Desktop or Web).
5. If the email or attachment(s) are password protected either;
    a. Phone the recipient, confirm their identify, then disclose the password
    b. Email the password separately

Personal email accounts must not be used for work purposes; all email can be accessed externally via the Office 365 Portal.

Emails relating to JTMAT must not be forwarded to personal emails addresses.

Student Accessible Areas

Personally identifiable, sensitive or confidential information must not be stored on areas that are accessible to students e.g. Student Shared Drives, Teams, SharePoint, Google Drive, Google Classroom; this includes but is not limited to names, address, grades, contact details and any other form of personal information. Students that have access to these areas could transmit this information to other parties without encryption.

In certain circumstances it may be necessary for students to save work in a location that is accessible to other students, this is permitted under this policy for this sole purpose.

Third Party Web Sites/Applications

Any web site that requires transmission of personal data including (but not exclusively) name, addresses, registration information, and timetable should only be accessed via HTTPS and have a valid SSL certificate. Do not access any website that presents a security certificate error.

All Trust websites that contain personal information are secured by certificates that encrypt the data in transit and validate the identity of the computer that is being connecting to.

If you are sending personal data to websites, the site must be reported to IT Services for it to be included in the Trust's Privacy Policy.

Multi Factor Authentication (MFA)

MFA provides a robust mechanism for preventing unauthorised access to systems and data and should be enabled if available. MFA is based upon the principles of "something you know" and "something you have" e.g. your password and a device.

All employees including long term supply and trainees are required to configure MFA.

Reporting

All employees and third parties should be aware of the following document: What should I do if I lose personal data?

Reporting a breach of this policy

If you suspect or know of a breach of this policy has occurred it must be reported immediately to the Trust's Data Protection Officer (DPO), either via email (dpo@jtmat.co.uk). Failure to report a breach could result in disciplinary action as defined in the Trust's disciplinary policy.

A record of each incident will be kept and updated by the DPO. If multiple breaches are recorded you may lose access to removable media or any other service that allows you to access sensitive or confidential data and the Trust may implement the disciplinary policy.

Reporting data loss

If data (encrypted or not) is lost it must be reported to the Trust's DPO immediately so a full internal investigation can take place. The DPO/IT Services/the Trust will follow the guidance set out by the ICO to manage the breach.

A record of each incident will be kept and updated by the DPO. If multiple breaches are recorded you may lose access to removable media or any other service that allows you to access sensitive or confidential data. In certain circumstances the ICO will be informed and the school may implement the disciplinary policy.

Reporting a concern or other issue

If you have any other concerns regarding this policy or its implementation contact IT Services or the Trust's Data Protection Officer either in person or via email (support@jtmat.co.uk/dpo@jtmat.co.uk) to discuss your concerns.

Data Recovery

When encrypting your USB memory stick, external hard disk or Windows mobile device, recovery information will be stored in Active Directory and is only viewable to IT Services. If you cannot remember a password to access a device this recovery information can be used to grant access and change the password.

If you have forgotten the password to a removable device contact IT Services in person with the device. ICT Support will then will record the request and take appropriate action.

Failure to comply

All persons named above (within the responsibilities section) are expected to fully comply with this policy, failure to do so can result in;

Employees

In the case of an employee the matter will be dealt with in accordance with the Trust's disciplinary policy.

Third Parties

In the case of third parties (as defined but not limited to the above) non-compliance will result in the immediate removal of access to the system. If damage or compromise of Trust' ICT systems or network results from non-compliance, the Trust will consider legal action against the third party. If data loss has occurred the matter may be reported to the Information Commissioners Office (ICO) after an internal investigation has taken place.

Liability

Please be advised that if an incident is reported to the ICO, liability and subsequently any fine or prosecution can be levied against an individual as well as the Trust. To find out more about the ICO's policy on enforcement visit: ICO Enforcement.