TKAT Information Security Encryption Policy

Date & Version	Action / Notes
Version 1	Governor ratification of policy to be minuted
Issued February 2018	Effective immediately

1. Purpose of the Policy

This policy is intended to establish the requirements for the application of encryption to data and equipment as a means of protecting the confidentiality, integrity and availability of TKAT's information assets. It also sets out any relevant standards which those controls must meet.

2. Scope

The policy covers the application of encryption to sensitive information at TKAT. As TKAT is a single legal entity, this is a single policy designed to be used across it's academies and offices.

3. Relationship with existing policies

This policy forms part of the TKAT Information Governance Framework. It should be read in conjunction with the Information Security Policy and Data Protection Policy.

4. Definitions

Sensitive Information: Information that is confidential, highly confidential or requires enhanced protection to ensure integrity or availability due to its nature. This may include, but is not limited to classified information, commercially sensitive information, personal data or special categories of data. Refer to the TKAT Data Protection Policy for more information on personal data or special categories of data.

Encryption: Encryption is the process of encoding information in such a way that only authorised parties can access it and those who are not authorised cannot. Encryption methods can be as simple as password protecting an office document (which scrambles the data until the password is re-entered to view it), or more complicated such as device encryption which is normally conducted by an IT Department.

Cryptographic: Cryptography is the practice and study of techniques for secure communication in the presence of third party adversaries.

5. Policy Statement

In order to mitigate the risk of disclosure or tampering with sensitive information through interception, loss or theft of data or equipment, TKAT shall deploy appropriate cryptographic security controls in conjunction with procedures that manage the associated encryption keys.

Where valid reasons exist, exceptions to this policy can be signed off by Senior Managers (i.e. academy SLT level or above), but must be done so in writing with the awareness of the TKAT IT Director.

6. Policy

6.1 Information

TKAT information and records shall normally be created and stored within a secure and managed system, as per TKAT's Information Security Policy.

However, when sensitive information are to be transmitted outside of such a secure system, it must be secured in transit so that it cannot be intercepted and read. This may include encrypting a file sent via email, encrypting a portable hard disk being used to transfer data or the use of encrypted transmission protocols such as SSL.

To ensure a secure link between users and servers, IT staff must make sure that all services which collect, process or transport personal data or sensitive information Eg; on-premises SharePoint, website forms, webmail etc is required to have SSL (Secure Socket Layer) version 3.0 or TLS version 1.2 level encryption.

Any costs associated with the use of encryption software must be borne by the relevant academy or central office.

6.2 Devices

When a device is capable of device encryption and recovery keys can be safely made available or stored by the IT Department, and the device is used to store sensitive information or personal data (as per the definitions in point 5.1) it is required that device encryption be applied.

Exceptions will apply where it can be clearly demonstrated that the device

1) is not mobile (that is, moved from office to office)
2) is securely stored at the end of every working day in a locked container.

6.2.1 Laptops

From the effective date of this policy, all TKAT laptops must be encrypted using full disk encryption unless exceptions apply under point 5.2

TKAT recognises that certain devices may be frequently cleared of sensitive information, and that these may be good candidates for an approved exception from the policy. Examples of such devices may include laptops used for examination purposes that are frequently re-imaged via existing well managed processes. TKAT requires the ability to decrypt a device in order to recover any information held upon it if necessary. TKAT and it's academies must therefore adopt encryption solutions shall manage any keys, passphrases or other secrets (for example, hardware tokens) necessary to recover data from encrypted devices.

In order to meet this policy, the encryption solution used to encrypt laptops shall be one of TKAT's approved solutions as set out in Schedule A.

6.3 Personally Owned Laptops

Personally owned laptops will not necessarily have security features enabled equivalent to business laptops. In addition they are likely to be used by a number of users, not all of whom may be TKAT staff and they are likely to be passed on to other family members, sold privately or recycled. In addition, being portable, they are at risk of being lost or stolen. As such these machines pose a high risk to the security of information they store.

Staff shall not create or store sensitive information on personally owned laptops, including via the use of file synchronisation tools without ensuring adequate security measures are in place including encryption where necessary. To ensure business continuity, non-sensitive TKAT information (e.g. working documents that do not contain sensitive information) shall not be stored on the device unless a copy is also stored in a TKAT owned system.

TKAT recognises that certain applications such as email or file synchronisation may automatically download information without a staff member's explicit action and therefore when such tools are used on personally owned laptops then encryption methods in line with those set out in Schedule A shall be applied. In addition the staff member must ensure that the laptop is protected in line with the IT security baselines. These include:

1) Up-to-date antivirus software
2) Up-to-date operating system patches
3) Up-to-date application patches

People handling TKAT Information take full responsibility for the application of security controls and for ensuring that information is secure throughout its lifecycle, which will include ensuring the device is securely wiped of TKAT information before disposal.

6.4 Smartphones and Tablets

All smartphones, tablets or other smart devices used for work purposes (regardless of ownership) shall be encrypted. In order to meet this policy requirement smartphones and tablets must meet the minimum technical specifications as set out in Schedule A.

When a user adds their work email to a mobile phone or tablet, they will be presented with a list of security measures that must be in place in order to use the email account on the device. Those measures will include encryption, minimum pass-code length, minimum idle time before locking the screen, and the ability to remotely wipe the device if lost or stolen.

Remote wipes will only be conducted upon notification from the staff member that the device has been lost, stolen, or where the staff member has taken the device or is accessing sensitive information without authorisation. TKAT will not be liable for any loss of data (e.g. text messages and photos) in the event of a remote wipe of the staff member's device.

6.5 Other Portable Devices

Particular care must be taken with the physical security of other portable devices with less inherent security features, such as USB sticks, external hard disks, digital cameras, and recording devices.

The use of these devices should be avoided for sensitive information. If they are absolutely required to collect or transfer sensitive information then that information shall not be stored on the device beyond the minimum length of time required to transfer that data to a secure location such as a secure laptop or on the local TKAT/academy network. Sensitive information stored on such a device, even temporarily, must be protected through either device encryption or file encryption. All sensitive information shall be securely deleted from the device immediately after successful transfer and the device must be either securely disposed of, or securely wiped when no longer required by TKAT.

6.6 Portable Devices used for Backup

Particular care must be taken with the physical security of other portable devices with less inherent security features, such as external hard disks which are used for long term storage, backup or archival purposes.

Whilst the device holds sensitive Information that information must be protected either with device encryption or file encryption, and the device must be disposed of securely, or securely wiped when no longer required by TKAT.

6.7 Other Devices

Where other equipment holds sensitive data, such as a multi-function devices (copiers), that equipment should be securely wiped before return to vendor or disposal.

6.8 Computer Workstations

TKAT owned workstations that run the managed workstation service image(s) provide a secure environment for people to work in. Such computers should also be encrypted when located in public facing areas, and where the device is of a small enough size to be at risk of theft.

6.9 Personally owned computer workstations

Personally owned workstations (i.e. desktop PCs and Macs) will not necessarily have security features enabled equivalent to managed TKAT owned workstations. In addition they are likely to be used by a number of users, not all of whom may be TKAT staff and they are likely to be passed on to other family members, sold privately or recycled. In addition, being located in a domestic setting they are at higher risk of being stolen. As such these machines pose a high risk to the security of information they store.

Staff shall not create or store sensitive information on personally owned workstations unless using appropriate remote technology (e.g. Office 365 online or Citrix). This includes via the use of file synchronisation tools (e.g. Dropbox, Google Drive and OneDrive). Non-sensitive information shall not be stored on a personally owned device unless a copy is also stored in a TKAT network drive.

TKAT recognises that certain applications such as email or file synchronisation may automatically download information without a staff member's explicit action and therefore when such tools are used on personally owned workstations then encryption methods in line with those set out in Schedule A shall be applied. In addition the staff member must ensure that the laptop is protected in line with the IT security baselines. These are:

1) Up-to-date antivirus software
2) Up-to-date operating system patches
3) Up-to-date application patches
4) Use of non-pirated and fully licensed operating system and applications

People handling TKAT Information take full responsibility for the application of security controls and for ensuring that information is secure throughout its lifecycle, which will include ensuring the device is securely wiped of TKAT information before disposal.

6.10 File Synchronisation and Sharing Tools

Staff must not put sensitive information at risk of compromise of confidentiality or any other proprietary TKAT information at risk of loss through the use of non-secure tools and methods (such as non-approved third party services) and/or personally owned email accounts. In particular, staff shall ensure that the use of any file synchronisation and sharing tool (for example, Dropbox, OneDrive and Google Drive) to support remote or mobile working is compliant with this and other TKAT policies. Refer to the IT Department for further clarification.

Encryption shall always be applied to TKAT sensitive information that transmitted to external services. The use of non-encrypted transfer methods such as FTP (File Transfer Protocol) are strictly prohibited.

6.11 Enhanced Security Requirements

TKAT recognises that specific functions may have enhanced requirements as a result of the information security requirements of their external partners (e.g. Welfare and transfer of information to the Local Authority). The IT Department must be notified of any such requirements, and will advise on the introduction of enhanced measures as needed.

6.12 Third parties

Where third parties are handling TKAT sensitive information, they must apply controls equivalent to those applicable to TKAT devices. Failure to do so may contravene the TKAT Data Protection Policy as well as this policy, and may put TKAT sensitive data at risk.

7. Responsibilities

Responsibility for reviewing the specific sets of controls to support this policy lies with the TKAT IT Director, and will be subject to annual review, taking account of changes in the internal and external environments and TKAT's appetite for risk.

Headteachers and Heads of central functions are responsible for ensuring that School/Department purchases meet the relevant specifications as set out in the Schedules. Where this is not acceptable for valid business reasons then Headteachers are responsible for signing off exceptions. Headteachers and Heads of central functions are also responsible for ensuring that staff are aware of the need to adhere to this policy and report non-compliance to the IT Department for advice and remediation.

Individual staff are responsible for adhering to the TKAT Information Governance Framework policies and following the relevant procedures. Where the policy requirements are reliant on individual staff taking steps to secure the information they are handling the individual staff member will be personally accountable and liable for failing to follow the required policy, procedure or process. Individual staff

are responsible for ensuring that any shortfalls in security controls are reported promptly to their line manager and (where an incident has occurred) to IT.

8. Compliance

Breaches of this policy may be treated as a disciplinary matter dealt with under TKAT's staff disciplinary policy as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract. The TKAT Data Protection Policy contains details on contract requirements which should be referred to before entering into an agreement.

SCHEDULE A – Encryption Specifications and Required Controls

TKAT Owned Laptop and Workstation Security Controls

TKAT owned laptops and workstations running Microsoft operating systems shall be encrypted using Bitlocker, VeraCrypt or Sophos SafeGuard. Other encryption tools must be vetted by the TKAT IT Security team.

Encryption standards should meet a minimum requirement of AES-256 encryption algorithm. Full disk encryption is required together with a complex boot password inclusive of at least eight characters in length, at least one uppercase character, one number and one symbol.

TKAT owned Apple laptops and workstations must have their user areas protected by FileVault encryption. Note that a strong device logon password is required.

Where any of the above controls cannot be adhered to for valid business reasons this shall be authorised in writing by the relevant Head of Department and a copy stored by the IT Team.

Access to, and advice on, the most appropriate encryption software and the necessary minimum technical computer specifications is available via the IT Team.

Personally Owned Laptop and Workstation Security Controls

Advice on the most appropriate encryption software is available via the IT Team.

TKAT is not able to provide licenses for the use of such software on personally owned devices and the staff member must ensure that they comply with licensing conditions.

All Smartphones and Tablets Basic Specification

Any smartphone or tablet intended for use for work must be capable of being encrypted. The versions of common software which will support this are:

- iOS 8 and upwards on iPhone 4S and later models (encrypted by default)
- Windows Phone 7 and later models (encryption must be enabled)
- Blackberry all versions (encryption must be enabled)
- Android 4.4 and later versions (encryption must be enabled)