Kemnal Technology College

TKAT

TKAT INFORMATION SECURITY POLICY

This Policy was reviewed:

July 2023

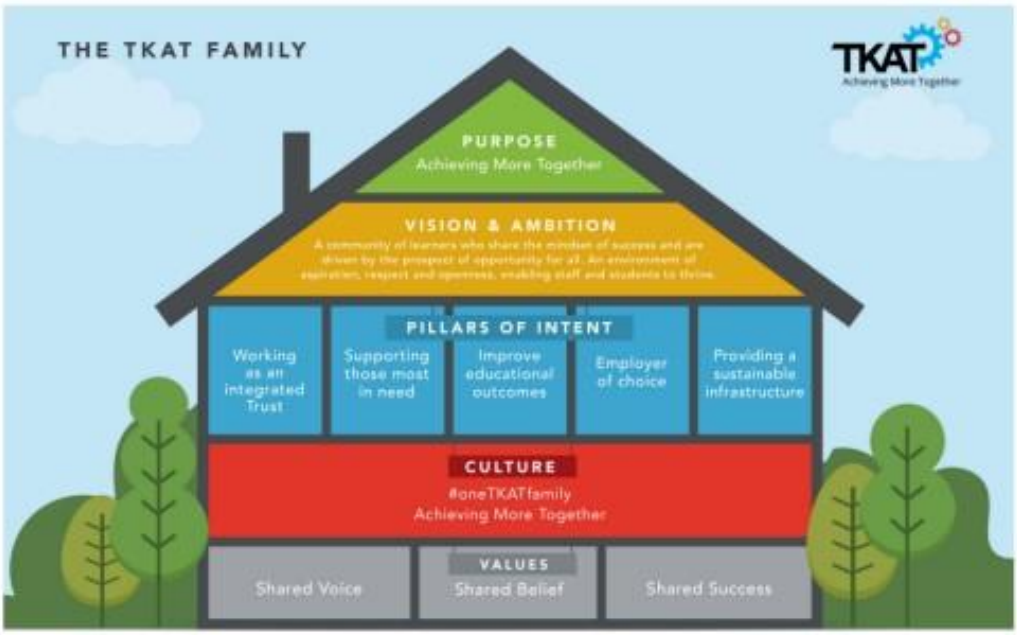
The Policy will next be reviewed by TKAT & Kemnal Technology College by:

March 2026

CONTENTS

VISION AND VALUES

The Kemnal Academies Trust (TKAT) aims to foster a culture of the highest professional standards in line with the Trust's purpose, vision and values.



PURPOSE OF THE POLICY

This policy is intended to establish the key principles and controls that TKAT will employ under ISO 27001. It is designed to protect the confidentiality, integrity, and availability of TKAT's information assets. It also sets out any relevant standards of which those controls must meet.

SCOPE

This policy applies to the entire TKAT organisation, inclusive of academies and is a single policy designed to reflect TKAT's commitment to effective information security.

RELATIONSHIP WITH EXISTING POLICIES

This policy forms part of the TKAT Information Governance Framework. It should be read in conjunction with the following policies:

- TKAT Data Protection Policy.
- TKAT Data Retention Policies
- TKAT Password Standards Policy
- Other legislation or regulations (including equal opportunities, audit, and ethics) affecting TKAT or its academies.

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.

Encryption: Encryption is a way of scrambling data so that only authorised parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as cipher text. Encryption methods can be as simple as password protecting an office document, or more complicated such as device encryption.

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

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 Director of IT & Data.

ACCESS CONTROL

Sharing Information

TKAT information and records shall normally be created and stored within a secure and managed system, such as Google Drive or Network servers.

When sensitive information is 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 but not limited to:

Drive sharing: Where possible a share link to a document or folder should be used to provide access to documents and folders without physically transferring them out of the trust secure systems. This minimises the transfer of data with the ability to control and revoke access at any point.

When sharing or creating Google Shared Drives, if the user is unsure of the access permissions and settings in Drive then it is essential to check with the IT Team first by emailing the IT Helpdesk. This will ensure that files and folders stored in the Drive are only accessible by the authorised users. Information on Google Permissions can be found in the TKAT Google Workspace Policy.

Email default: When email is sent/received via the Gmail app it is encrypted using S/MIME to support enhanced encryption in transit and automatically encrypts your outgoing emails if it can.

Email confidential mode: By selecting 'Confidential mode' Gmail replaces message content and attachments with a link to the content.

Email advanced encryption solutions: 3rd party encryption solutions should be used to control the access of confidential emails at any time after the emails have been sent. Virtru solution is used by TKAT, which works within the native Gmail environment. Any costs associated with the use of encryption software must be borne by the relevant academy or central office.

3rd Party Software Solutions: Where staff or student data is being transferred, shared or made accessible to third parties, academies must ensure that:

- Data Processing Agreement (DPA) has been completed for 3rd party companies processing personal and sensitive data. This must be managed by the Privacy Champion and approved by the TKAT DPO
- Data Protection Impact Assessment (DPIA) has been completed for 3rd party companies accessing personal and sensitive data. This must be managed by the Privacy Champion and approved by the TKAT DPO

File Transfer or Sharing: *The use of file sharing websites or file transfer protocol solutions is not permitted unless approved The IT Department must be notified of any such requirements, and will advise on the introduction of enhanced measures as required.*

Confidential or sensitive data must not be saved or transferred via portable hard disks or USB storage devices.

Device Encryption

It is required that device encryption must be applied to all devices that are capable of, to protect sensitive information or personal data (as per the definitions in point 3 of the Data Protection Policy). Where the device does not have this capability it must be managed via a MDM (Mobile Device Management) solution to allow the device to be secured and wiped in the event of it being lost or stolen

Exceptions will apply where it can be clearly demonstrated that the device does not need security measures, i.e. the device is not mobile (that is, moved from office to office)

Computer Workstations: All TKAT workstations 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.

Laptops: All TKAT laptops must have installed, and be encrypted with, Bitlocker (Windows encryption technology).

Chromebooks: All TKAT Chromebooks must be enrolled onto the TKAT Google Workspace. This ensures they can be managed remotely. All Chromebooks are encrypted by default.

Android Tablets: All TKAT Android tablets must be managed via a MDM solution - TKAT uses Hexnode MDM. They must have the encryption setting option enabled.

Apple iPads: All TKAT iPads must be managed via a MDM - TKAT uses JAMF. They must have at least a pin code activated as minimum security - this action immediately encrypts the data.

Mobile Phones: All Mobile phones must be managed by an MDM. To encrypt the data either:

- Apple iPhone: They must have at least a pin code activated as minimum security - this action immediately encrypts the data
- Smartphones: They must have the encryption setting option enabled

Staff, Governor, Trustee and Members Personal Devices: Staff should not use their personal device (e.g. Laptop, Chromebook, MacBook) at work. All staff should be provided with suitable equipment required for their role. This ensures the encryption and security of data is maintained as stated in 6.2.1-6.2.5.

- Exclusions:
  - Staff may be required to log into work accounts on personal devices at home, or on mobile phones. If this is required, and in line with the 'Code of Conduct' and 'Acceptable Use of IT' Policies, staff are responsible for signing out of the accounts/device when unsupervised and ensuring the device has a secure method to login. They must ensure that they do not download or transfer any

sensitive data from the account they have logged into.

- Governors, Trustees and Members may be required to use their own device, but all governors must be provided with a TKAT Google account. This allows all communications and document storage to be kept with the secure Google Workspace ecosystem

Device Wiping

There are certain parameters that will require hardware to be wiped of all data, these include but are not limited to:

- Re-image or installation of an Operating System
- Clear large storage volumes preventing the device from performing efficiently
- Remove potential security breaches such as Ransomware or Malware
- Disposal of the hardware (see Device Disposal)

As such, it is essential that the user ensures that their data is stored in the correct location that is either being backed up, or is stored in a cloud solution. Any data stored on the device itself may not be recoverable.

Device Disposal

All hardware must be disposed of through a TKAT approved contractor. All approved contractors are appointed on the basis that they comply with ISO 9001, 14001, 27001, ensuring that all information stored on the hardware is securely wiped at the end of its TKAT life. Evidence of all WEEE disposal certificates must be added to the asset register of each device. This includes the disposal of devices such as a Multi-function device (photocopiers) and Telephony equipment, whereby any new installation will include safe disposal of legacy hardware.

Information Backup

All sensitive and personal data must be backed up securely in the cloud to ensure that any data that is lost, stolen or damaged can be recovered in a timely manner to ensure minimal impact on the day to day running of the business and education of the children.

All backups must be fully encrypted using cryptographic methods to maintain the integrity of the data being backed up. If on-site backups are used they must also be encrypted and stored in a different and secure location to that of the primary source of data that is being backed up.

INFORMATION CLASSIFICATION

Information Access Levels

When sharing information, it is essential to assess the level of access required. In order to assess this, two questions need to be asked:

- What is the person(s) role responsible for?
- What does the person(s) role require access to?

Information and the level of access should only be given if it is relevant to the person. The levels shouldn't be based on employees' seniority but on the information that's necessary to perform certain job functions.

Access Classification

All data assets owned by the academy and/or trust must be classified in order to both grant and monitor who has access to the information. The four categories are:

- Confidential (only senior management have access)
- Restricted (some employees have access)
- Internal (all employees have access)
- Public information (everyone has access)

Handling of Information

The table below outlines expected practice to securely manage information based on its classification. The list is not exhaustive, if you require further assistance please contact the TKAT Data Lead for further guidance.

	Paper files *It is advised to use digital storage where possible*	**Digital Files** *It is advised to move all digital files to secure Google Shared Drives, not Google My Drive*	**Email**
Confidential *e.g. Staff payroll*	• Kept onsite in secure lockable storage at all times • Post only if essential via signed for and tracked service • Stored for retention in secured areas • Dispose of securely by shredding	• Kept in Google Shared Drive or secure network storage • Shared with Senior roles only • Transferred only via methods stated in 6.1.1, 6.1.4 and 6.1.5 • Stored in retention protected drives • Deleted from storage and backup when no longer required	• Sent only via methods stated in 6.1.4 • Advised to share from Google Drive or as a link in an email
Restricted *e.g. EHCP, Safeguarding records*	• Stored in secure offices available to authorised staff • Post only if essential via signed for and tracked service • Stored for retention in secured areas • Dispose of securely by shredding	• Kept in Google Shared Drive or secure network storage • Shared with Senior roles and role specific only • Transferred via appropriate method stated in 6.1 • Stored in retention protected drives • Deleted from storage and backup when no longer required	• Sent only via methods stated in 6.1.3, 6.1.4 and 6.1.5 • Advised to share from Google Drive or as a link in an email
Internal *e.g. Pupil assessments*	• Stored onsite in files, drawers or cupboards to restrict access by guests and visitors • Disposed of securely by shredding	• Kept in Google Shared Drive or network storage • Shared with most staff roles within TKAT only • Transferred via appropriate method stated in 6.1 • Deleted from storage and backup when no longer required	• Sent only via methods stated in 6.1.4 and 6.1.5 • Advised to share from Google Drive or as a link in an email
Public *e.g. Policies*	• Relevant storage based on the document • May be used for display purposes • Disposed of in paper recycling	• Kept in public view Google Drives • Links may be used to websites or used for digital signage • Deleted when no longer required	• Sent via normal email methods

STAFF AWARENESS TRAINING

Staff training will be delivered through a variety of ways outlined below:

- **Annual refresher training:** Accessed through TKAT's online training portal, all staff are expected to complete refresher training courses. Aimed at reminding staff of key points and raising awareness of what good practice looks like. These courses will cover both 'Cyber Security' and 'Data Protection' with an increasing complexity for staff who have roles with responsibilities in these areas.
- **Bespoke school training:** Upon request of the school, specific training can be arranged covering both generalised or specific areas within cyber-security and data protection to ensure best practice across the academy for information security and management. Please contact the TKAT Data Lead to discuss.
- **Ad Hoc training requests:** At times staff may request refresher training to either remind or develop them around areas of information security. TKAT actively encourages these requests to ensure staff have the necessary skills to carry out their role.
- **National Awareness days/weeks:** Throughout the year, national awareness days/weeks offer a good opportunity to promote and remind staff of best practice. This is typically done by sharing activities and checks around their own data security and information management practice.

RESPONSIBILITIES

TKAT IT & Data Team

- IT & Data Leadership team will continue to review processes and policies to ensure they are up to date and fit for purpose to keep all information relating to staff and children in TKAT safe and secure.
- IT Technician teams will ensure devices, digital storage and software solutions settings comply with the requirements stated in this policy
- Regularly monitor and quality assure settings and permissions on drives and docs and inform the staff or academies if any insecurities are found

Corporate Staff, Academy Staff, Governors and Trustees

- Complete the annual refresher training
- Actively participate in any activities or checks promoted through the awareness events across the trust
- Review their own practices to ensure information security is maintained
- Actively support and remind colleagues they work with if information security practice needs to be improved
- Report any known breaches of this policy or where they believe information security practice is not acceptable

Academy Leaders

- Responsible for ensuring that all staff:
  - are aware of the need to adhere to this policy
  - report non-compliance to the IT Department for advice and remediation
  - Complete the required annual refresher training
- Headteachers are responsible for signing off exceptions after consultation with the Director of IT & Data.

Privacy Champions

- Monitor and review information security practices across the academy
- Lead, monitor and organise the training for all staff
- Ensure the academy remains compliant to all areas outlined in this policy
- Liaise with TKAT Data team and the DPO to continually improve practice and processes

Data Protection Officer

- Record any information data breaches and report to the ICO as required
- Act as the consultant to the trust to continually review and improve practice and processes to ensure the information management is fit for purpose
- Lead training for Privacy Champions
- Ensure that TKAT, as a trust, and its individual academies demonstrate compliance with the GDPR.

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 in a 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.