TKAT Information Security 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 general themes and controls that TKAT will employ to protect the confidentiality, integrity and availability of TKAT information.

1. Scope of the Policy

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.

2. Responsibilities

The Board of Directors and management of TKAT, are committed to preserving the confidentiality, integrity and availability of all physical and electronic information assets throughout the organisation. This is in order to preserve its financial, legal, regulatory and contractual compliance as well as its reputation. Information and information security requirements will continue to be aligned with TKAT's goals and the The TKAT Information Governance Framework is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

3. Relationship with Existing Policies

This policy has been drawn up within the context of:

1. TKAT Data Protection Policy;
2. TKAT Information Security Encryption Policy; and
3. Other legislation or regulations (including equal opportunities, audit and ethics) affecting TKAT or its academies.

4. Governance

TKAT's current strategic plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of corporate risk register.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems, encryption standards and information security incident reporting are fundamental to this policy.

TKAT aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk register.

The TKAT Information Governance Framework is subject to continuous, systematic review and improvement.

The IT Director will periodically review the security policy, in line with technological advancements and as a result of compliance requirements.

This policy will be reviewed to respond to any changes in the risk assessment process or TKAT's risk management process.

5. Compliance

All Employees/Staff of TKAT are expected to comply with this policy. All Employees/Staff, and certain external parties, will receive appropriate training on cyber security and data protection. Any breach of this policy may result in disciplinary proceedings or further action in the case of agreements with third parties.

TKAT is committed to achieving Cyber Essentials certification and compliance with UK data protection regulation.

6. Policy

In this policy, 'information security' is defined as ***'preserving the confidentiality, integrity and availability of physical and information assets'.***

This means that management, all full time or part time Employees/Staff, subcontractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in mandatory training or contractual arrangements) to preserve information security, to report security breaches and to act in accordance with the requirements of the TKAT Information Governance Framework. All Employees/Staff will receive information security awareness training.

6.1 Confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorised access to TKAT's information and systems . This includes but is not limited to its networks, network drives, websites, extranets, and information management systems.

6.2 Integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency at each academy or corporate office, including for network(s), website(s), extranet(s) together with data backup plans and security incident reporting. TKAT and its academies must comply with all relevant data-related legislation including the EU General Data Protection Regulation.

6.3 Availability

This means that information and associated assets should be accessible to authorised users when required whilst remaining physically secure. The computer network must be resilient and the academy/corporate office must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must also be appropriate business continuity plans.

6.4 Physical Assets

This refers to physical assets of TKAT and its academies including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

6.5 Information Assets

Information assets in the scope of this policy include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and tablets, as well as on CD ROMs, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc). of TKAT.

7. 3rd Party Processors

TKAT as a controller, will only instruct processors (e.g. suppliers and service providers) to process personal data on its behalf where processors have adequate technical and organisational measures in place to protect the confidentiality, integrity and availability of personal data. Processors must undergo annual assurance monitoring and in the case of a new Processor, a Data Protection Impact Assessment (DPIA) if the processing activity warrants it. Refer to the Data Protection Policy for further information.

8. Access Control

Access control is a security technique that can be used to regulate who or what can view or use the resources of an organisation.

There are two main types of access control: physical and logical. Physical access control limits access to sites, buildings, rooms and physical IT assets. Logical access limits connections to computer networks, system files and data.

TKAT has adopted the following access control principles:

- TKAT controls access to information on the basis of operational and security requirements.
- Access control rules and rights must be agreed at the design phase of any project regardless of size where that project includes the setup of processes which handle personal or sensitive data
- When deciding which access rights to apply, staff must take into account:
    - Premises access control – so that unauthorised persons are prevented from gaining physical access to premises, buildings or rooms where personal or sensitive data is being processed.
    - System access control – access to data processing systems is prevented from being used without authorisation.
    - Data access control – ensuring that persons entitled to use a data processing system gain access only to the data to which they have a right of access.
    - Ensuring that personal data cannot be read, copied, modified or removed without authorisation.
- Staff must also take into account data protection regulations and contractual commitments regarding access to data or services.
- The ‘need-to-know’ principle must always be applied i.e. access is granted at the minimum level necessary for the role.
- Regarding computer networks, management of access rights is also completed using the need-to-know principle, and wherever possible, network segmentation is to be used.
- User access requests must be subject to formal authorisation, to periodic review and removal when appropriate.

9. Security Breaches

A security breach is any incident or activity that causes, or may cause, a break down in the confidentiality, integrity or availability of the physical or electronic information assets of TKAT. Data breaches are a serious type of security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Any security breaches should be reported immediately to the TKAT IT Director, even if the facts are not fully known. Data breaches shall be treated as per the Data Breach Notification Procedure and in compliance with the Data Protection Policy.

10. Summary of relevant legislation

- The Computer Misuse Act 1990
- Data Protection Act 1998
- General Data Protection Regulation 2018
- Data Protection Bill 2018
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Defamation Act 1996
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Criminal Justice and Immigration Act 2008
- Terrorism Act 2006
- Counter-Terrorism and Security Act 2015 – Statutory Guidance