KALEIDOSCOPE
Multi Academy Trust

TECHNICAL SECURITY POLICY

Based upon the Support Services in Education model policy

Approved by:	Kaleidoscope Trust Board
Last reviewed on:	November 2023
Next review due by:	November 2025

Contents

Contacts and Review Information

Data Protection Officer	Amy Brittan aybrittan@somerset.gov.uk
School Data Protection Lead	Simon Marriott office@kaleidoscopemat.co.uk

Introduction

1.1 Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Kaleidoscope Multi-Academy Trust and its schools will be responsible for ensuring that its infrastructure/networks are as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring or business continuity purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and this has an impact on policy and practice
- there is an up-to-date Business Continuity and Disaster Recovery Plan including the KMAT Cyber Response Plan which details our response to a major cyber incident such as a ransomware attack which could significant impact a school's ability to deliver education, run the school site, and safeguard learners

- KMAT has a contract with 2IT to provide support for technical security
- It is the responsibility of the Trust to ensure that 2IT is fully aware of KMATs online safety policy/data protection/acceptable use agreements. The Trust and its schools should also check that their managed service provider is following up-to-date guidance and advice from the National Cyber Security Centre https://www.ncsc.gov.uk/section/advice-guidance/all-topics

Scope of the policy

2.1 This policy should be read alongside the following documents:

- Business Continuity Plan
- Risk Register
- Data Protection Policy
- Online Safety Policy
- Cyber Response Plan

- Safeguarding Policy
- Privacy notices for pupils/parents

2.2 This policy reflects the requirements of KMAT and its schools to comply with the following legislation

- The UK General Data Protection Regulation
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- Keeping Children Safe in Education 2022

2.3 This policy applies to all staff including school, agency staff, contractors, work experience students and volunteers

Responsibilities of the Trust/Academy/School

KMAT and its schools will:

3.1 be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented

3.2 ensure that the relevant people receive up-to-date guidance (e.g. from the National Cyber Security Centre) and training and are effective in carrying out their responsibilities

3.3 ensure that technical systems are managed in ways which meet recommended technical standards of the Department for Education https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges

3.4 ensure that there are regular reviews and audits of the safety and security of the Trusts technical systems (see Section 12 Monitoring)

3.5 ensure that servers, wireless systems and cabling are securely located and physical access restricted

3.6 ensure that appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of KMAT and its schools' systems and data

3.7 ensure that responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff

3.8 by liaison with 2IT, ensure that all users have clearly defined access rights to the Trusts technical systems

3.9 by liaison with 2IT, ensure that details of the access rights available to groups of users are recorded by 2IT and are reviewed, at least annually, by the senior leadership team

3.10 by liaison with 2IT, ensure that an appropriate system is in place for users to report any actual/potential technical incident to the nominated in-school lead

3.11 by liaison with 2IT, ensure that an agreed policy is in place and implemented regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on Trust/school devices that may be used out off site

3.12 by liaison 2IT, ensure that an agreed policy is in place and implemented regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on KMAT and its schools' devices

3.13 by liaison 2IT, ensure that the Trust infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.

3.14 by liaison with the network manager/technical support provider, ensure that any cyber incidents are reported to the relevant authorities e.g. Action Fraud

Responsibilities of 2IT

4.1 The responsibilities of 2IT are primarily listed in the contract with the provider.

4.2 In addition to the other requirements of this policy, 2IT will:

- Read, sign, and follow the Trust Acceptable use Agreement for technicians
- regularly monitor and record the activity of users on the school's technical systems (add details of the monitoring programs that are used)
- ensure that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations (Inadequate licensing could cause the Trust and its schools to breach the Copyright Act which could result in fines or unexpected licensing costs)
- ensure that remote management tools are used by staff to control workstations and view users' activity
- ensure that mobile device security and management procedures are in place (where mobile devices are allowed access to systems).
- ensure provision for temporary access of "guests", (e.g., trainee teachers, supply teachers, visitors) onto school systems
- enforce the Trust agreed policy regarding the downloading of executable files and the installation of programs on school devices by users

Responsibilities of staff

5.1 This policy applies to all staff including school, agency staff, contractors, work experience students and volunteers.

KMAT staff will:

- read, sign, and follow the Trusts Acceptable Use Agreement
- read and follow the KMAT Data Protection policy
- complete the National Cyber Security Centre's online staff training and maintain an awareness of the common types of security risks such as phishing and scam emails
- ensure that school devices are locked when the staff member is out of the room
- ensure that passwords for school systems are not shared with other staff members or students
- if using removable storage (laptop, tablet, USB memory stick) ensure that this is approved by the school, and is password protected and encrypted
- when working from home, ensure appropriate security is in place to protect equipment or information not be used by non-school staff. This will include ensuring equipment and information is kept out of sight
- ensure that any machine not routinely connected to the school network, is brought in regularly to receive updates by the IT team
- ensure that all school data is stored on the school network or portal, not kept solely on the laptop
- ensure that all locally stored data is synchronised with the school network server on a frequent basis
- ensure that school-issued laptops are available for inspection by school-authorised personnel (e.g. the network manager) at any time
- not attempt to access any network drives or areas to which they do not have authorised permission from the school
- not attempt to by-pass security to download apps or .exe files without the prior permission of the school
- use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code
- **in the event of a suspected cyberattack.** turn off device and inform the school office and do not connect device to the school network until it has been checked by 2IT technician

Network/Server security

6.1 Servers are physically located in an access-controlled environment. Unrestricted access to the computer facilities is confined to designated staff whose job function requires access to that particular area/equipment

6.2 Restricted access may be given to other staff or third-party support where there is a specific job function need for such access

6.3 The most recent security patches are installed on the system as soon as practical. The only exception being when immediate application would interfere with business requirements

6.4 Servers will have security software (Anti-Virus and Anti-Spyware) installed appropriate to the machine's specification and in line with current recommendations from the National Cyber Security Centre https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software

6.5 Servers will always be password protected, and locked when not in use

6.6 Users will not be able to download apps or .exe files without the prior permission of the school and network manager/technical support provider

6.7 Security-related events should be reported to the IT team and to the DPO. Corrective measures will be prescribed as needed. Security-related events could include, but are not limited to, port-scan attacks, evidence of unauthorised access to privileged accounts

6.8 IT infrastructures such as routers, switches, wireless access points etc. should be kept securely and only be handled by authorised personnel

6.9 Backup Procedures:

- Backup software must be scheduled to run routinely, as required, to capture all data as required
- Backups should be monitored to make sure they are successful
- A test restoration process will be run regularly and at least annually (see Section 12 Monitoring)
- Backup media must be securely stored in a fireproof container
- Backup media stored off-site must be transported and stored securely

Workstation security

12.1 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorised users, including:

- restricting physical access to workstations to only authorised personnel

- securing workstations (screen lock or logout) prior to leaving area to prevent unauthorised access
- enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
- complying with all applicable password policies and procedures
- ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- ensuring workstations are used for authorised purposes only
- never installing unauthorised software on workstations
- storing all confidential information on network servers
- keeping food and drink away from workstations in order to avoid accidental spills

Password security

Staff passwords

8.1 All KMAT networks and systems are protected by secure passwords.

8.2 When working away from the school, staff will use multi-factor authentication to access the school's online resources.

8.3 All users have clearly defined access rights to technical systems and devices. Details of the access rights available will be reviewed, at least annually, by the senior leadership team as detailed in Section 3.9

8.4 All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

8.5 Passwords must not be shared with anyone

8.6 Passwords should be long. Good practice highlights that passwords over 12 characters in length are more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack

8.7 Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school

8.8 Passwords must not include names or any other personal information about the user that might be known by others

8.9 Passwords must be changed on first login to the system

8.10 Passwords should not be set to expire as long as they comply with the above but should be unique to each service the user logs into.

Learner passwords

8.11 Foundation Stage and KS1 learners will have simple passwords with a six-character maximum, without special characters

8.12 Records of learner usernames and passwords for Foundation Stage/KS1 pupils can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.

8.13 Password requirements for learners at Key Stage 2 and above will increase as pupils progress through the school

8.14 All learners will be required to change their password if it is compromised. Passwords will not be regularly changed but should be secure and unique to each account.

8.15 Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Administrator passwords

8.16 Each administrator will have an individual administrator account, as well as their own user account with access levels set at an appropriate level. These accounts will have multi-factor authentication in place

8.17 Administrator passwords for the school systems should also be kept in a secure place e.g., school safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account. (A school should never allow one user to have sole administrator access)

8.18 If the school uses any password manager tools for storing administrator passwords, they must follow the guidance from the National Cyber Security Centre on password manager solutions https://www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide

Setting and resetting passwords

8.19 It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.

8.20 Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the network manager / school technician or an administrator who is easily accessible to users. The password generated by this change process should be system generated and only known to the user. This password should be temporary, and the user should be forced to change their password on first login. The generated passwords should also be long and random

8.21 Where automatically generated passwords are not possible, then an age-appropriate password generator e.g. www.dinopass.com or https://passwordsgenerator.net should be used to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary, and the user should be forced to change their password on the first login

8.22 Requests for password changes should be authenticated by the network manager / school technician or an administrator who is easily accessible to users to ensure that the new password can only be passed to the genuine user

8.23 Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. (For example, providing a pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)

8.24 In good practice, the account is "locked out" following six successive incorrect log-on attempts

8.25 Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption)

Awareness and training

9.1 It is essential that users are aware of the need to keep the school's systems safe from harm

9.2 This will be done at an age-appropriate level e.g., for young learners, staff will talk about the importance of keeping your password safe (see the Online Safety policy for further details). Key Stage 2 learners will complete the National Cyber Security Centre's CyberSprinters activity https://www.ncsc.gov.uk/collection/cybersprinters . Key Stage 3 and 4 learners may participate in the CyberFirst programme https://www.ncsc.gov.uk/cyberfirst/overview

9.3 Staff will complete the National Cyber Security Centre Top Tips for staff training (see para 5.1)

9.4 It will also be done through staff modelling appropriate use e.g., not leaving devices logged on, and not sharing passwords with classroom assistants

9.5 Members of staff will be made aware of this policy:

- at induction
- when logging onto the school network
- through the online safety policy and password security policy
- through the acceptable use agreement

9.6 Learners will be made aware of this policy:

- when logging onto the school network (via an age-appropriate login message)
- in lessons (e.g. online safety lessons)

- through the acceptable use agreement

Disposal of Redundant ICT Equipment

10.1 All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

10.2 All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. If the storage media has failed it will be physically destroyed. KMAT and its schools will only use authorised companies who will supply a written guarantee that this will happen.

10.3 Disposal of any ICT equipment will conform to:

- the Waste Electrical and Electronic Equipment Regulations 2018
- the UK GDPR and Data Protection Act 2018
- the Electricity at Work Regulations 1989

10.4 The schools will maintain a comprehensive inventory of all its ICT equipment including a record of disposal. This will include:

- Date item disposed of
- Authorisation for disposal, including: verification of software licensing, any personal data likely to be held on the storage media
- How it was disposed of e.g. waste, gift, sale.
- Name of person and/or organisation who received the disposed item.

10.5 Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Reporting policy incidents

11.1 Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data should raise the matter with the Headteacher/Executive Headteacher/Head of School

Monitoring and evaluation

12.1 This policy will be monitored and reviewed every 2 years or sooner if legislation changes

12.2 KMAT and its schools will monitor the implementation of the policy through:

- maintaining an up-to-date business continuity plan that reflects the latest risks to education settings following advice from the National Cyber Security Centre
- checking the school's technology standards against the latest DfE guidance https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges
- annual data protection walks around the school site to ensure that the school's requirements are followed by staff
- annual back-up and restore check of data
- regular spot checks of school systems and devices
- checks against national cyber security auditing systems e.g. the Cyber Essentials scheme About Cyber Essentials - NCSC.GOV.UK

November 2023