December 2023

# Kings Academy Trust – Cyber Security Principles

The DfE Cyber Security Standards for Schools were updated on 10th October 2022 and these new cyber standards should be met by schools as soon as possible.

1. Protect all devices on every network with a properly configured boundary or software firewall. Properly configured firewalls prevent many cyber-attacks.

2. Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date. Using the security features that devices already have is the most basic form of cyber security.

3. Accounts should only have the access they require to perform their role and should be authenticated to access data and services. Successful cyber-attacks target user accounts with the widest access and highest privileges on a network.

4. Protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication. Multi-factor authentication is especially important if an account has access to sensitive or personal data.

5. Anti-malware software should be deployed to protect all devices in the network, including cloud-based networks. Up-to-date anti-malware and anti-virus software reduces the risk from many forms of cyber-attack.

6. Administrators should check the security of all applications downloaded onto a network. Applications can insert malware onto a network or have unintentional security weaknesses.

7. All online devices and software must be licensed for use and should be patched with the latest security updates. Hackers try to identify and exploit the vulnerability that each new security update addresses.

8. There should be at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site. If all copies were held in the same location, they would all be at risk from natural disasters and criminal damage. KATs backup system is stored at 2 UK based server farms.

9. Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber-attack. Being unprepared for a cyber-attack can lead to poor decisions, slow recovery, and expensive mistakes. This will be carried out by an independent company on a yearly basis.

10. Serious cyber-attacks should be reported. Cyber-attacks are crimes against a school that need to be investigated so perpetrators can be found and counter-measures identified.

11. You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation. The protection of sensitive and personal data is vital to the safety of staff and students, and the reputation and confidence placed in schools.

12. Train all staff with access to school ICT networks in the basics of cyber security. The most common forms of cyber-attack rely on mistakes by busy staff members to be successful.

In order to achieve these standards, The Central Executive Team and establishments in the Trust will need to ensure they have robust policies and procedures covering:-

- Filtering
- Anti-virus
- Malware and Ransomware
  (the items above must be secure at both infrastructure level and across all devices)
- Back-ups and Data Recovery including knowledge of when / where these are taken, their physical locations, and retention periods
- Data Interchange via third party carriers; e.g. Wonde and Groupcall and other stakeholders / agencies; e.g. Awarding Bodies and LAs
- Telephony including identifying 'fake numbers' where the technology available allows
- Testing the Resilience and Security of networks and online content
- Business Continuity in the event of a mission critical breakdown or malicious attack