Cyber Security Policy

For the Following Academies:

Holy Trinity C of E Primary School
Connaught Junior School
Crawley Ridge Infant School
Crawley Ridge Junior School
Windlesham Village Infant School

This Cyber Security Policy was approved and adopted by the Trust Board in Aut 2023
It will be reviewed in Aut 2024

Contents:

Statement of Intent

The Alliance Multi Academy Trust (TAMAT) is committed to maintaining the confidentiality, integrity, and availability of its information and ensuring that the details of the finances, operations and individuals within the Trust are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

The Trust recognises that breaches in security can occur. In schools, most breaches are caused by human error, therefore all staff should know how to minimise the risk. In addition, because most information is stored online or on electronic devices that can be vulnerable to cyber-attacks the Trust will make sure there are procedures in place to prevent attacks occurring. To minimise both risks, it is necessary to have a contingency plan containing a procedure to minimise the potential negative impact of any security breach, to alert the relevant authorities and to take steps to prevent a repeat occurrence.

1. Legal Framework

This Policy has due regard to all relevant legislation and guidance including, but not limited to the following:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ESFA (2022) 'Academy Trust Handbook 2022'

This Policy operates in conjunction with the following Trust Policies:

- Data Protection Policy
- Staff Code of Conduct
- Disciplinary and Capability Policy
- Cyber Response and Recovery Plan
- Local Academy Policies (Acceptable Use, Behaviour, and others)

2. Types of Security Breaches and Causes

Unauthorised use without damage to data - involves unauthorised persons accessing data on the school system, e.g., hackers who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it. This includes unauthorised people within the school, e.g., schools where pupils access systems that staff have left open and/or logged into, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

Unauthorised removal of data – involves an authorised person accessing data, who removes the data to pass it onto another person who is not authorised to view it, e.g., a staff member with authorised access who passes the data to a friend without authorised access. This is also known as data theft. The data may be forwarded or deleted altogether.

Damage to physical systems – Involves damage to hardware in the school/Trust IT system, which may result in data being inaccessible to either or both but can be accessed by unauthorised persons.

Unauthorised damage to data – Involves an individual person causing damage to data, either by altering or deleting it. Data may also be damaged by a virus attack, rather than a specific individual.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence.

- Accidental breaches can occur because of human error or insufficient training for staff, so they are unaware of the procedures to follow.
- Malicious breaches can occur because of a hacker wishing to cause damage to the school through accessing and altering, sharing, or removing data.

Breaches caused by negligence can occur because of a staff member knowingly disregarding School/Trust Policies and procedures or allowing pupils to access data without authorisation and/or supervision.

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the school/Trust software more vulnerable to a virus.
- Incorrect firewall settings being applied, e.g., unrestricted access to the school network, can allow unauthorised individuals to access the school system.
- Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten.

3. Roles and Responsibilities

The TAMAT Trust Board will be responsible for:

- Ensuring the Schools/Trust has appropriate cyber-security measures in place.
- Ensuring the Schools/Trust has an appropriate approach to managing data breaches in place.
- Support relevant staff in the delivery of the Policy.

The Headteacher will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Schools' Online Safety Policy and Procedures.
- Organising training for staff members in conjunction with the online safety officer.

The DPO will be responsible for:

- The overall monitoring and management of data security.
- Deciding which strategies are required for managing the risks posed by internet use.
- Leading the Trust response to incidents of data security breaches, including leading the cyber recovery team.
- Assessing the risks to the school in the event of a cyber-security breach.
- Ensuring a log of cyber-security incidents in maintained.

- Producing a comprehensive report following a full investigation of a data security breach.
- Determining which organisations need to be notified following a data security breach, and ensuring they are notified.
- Working with IT Support after a data breach to determine where weaknesses lie and improve security measures.
- Keep up to date with data security, network security and preventing breaches.
- Monitor and review the effectiveness of this policy and communicating any changes to relevant staff.

The DSL will be responsible for:

- Assessing whether there is a safeguarding aspect to any cyber-security incident and considering whether any referrals need to be made.

All members of staff will be responsible for:

- Understanding their responsibilities regarding this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

4. Secure Configuration

An inventory will be kept of all ICT hardware and software currently in use across the Trust, including mobile phones and other personal devices provided by the school/Trust. The inventory will be stored in the central office and will be audited on a termly basis to ensure it is up to date. Any changes to the ICT hardware will be documented using the inventory and checked before use.

Systems should be audited on a termly basis by IT Support to ensure the software is up to date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security and will be recorded in the inventory. Any software that is out of date or reaches its 'end of life' will be removed from systems e.g., when suppliers end their support for outdated products, meaning that the product is not able to fulfil its purpose anymore.

All hardware, software and operating systems will require passwords from individual users. Passwords will be changed regularly to prevent access to facilities which could compromise network security. In line with Trust regulations 2 step authentication will be used when accessing software when not in the TAMAT tenancy.

TAMAT will consider referring to the five security controls outlined in the National Cyber Security Centre's (NCSC's)- Cyber Essentials. These are:

Firewalls: Firewalls function as a barrier between internal networks and the internet. They will be installed on any device that can access the internet, particularly where staff are using public or otherwise insecure Wi-Fi.

Secure Configuration: The default configuration on devices and software are often as open as possible to ensure ease of use, but they also provide more access points for unauthorised users. The Trust will remove or disable any unnecessary functions and change default passwords to reduce the risk of a security breach.

Access Control: The more people have access to data the larger the chance of a security breach. The Trust will ensure that access is given on a 'need to know' basis to help protect data. All accounts will be protected with strong passwords and two-factor authentication (where needed).

Malware Protection: The Trust will protect itself from malware by installing antivirus and anti-malware software and using techniques to protect any malware issue.

5. Network Security

In line with UK GDPR, the Trust will appropriately test, assess, and evaluate any security measures put in place regularly to ensure these measures remain effective.

Each school will employ firewalls to prevent unauthorised access to the systems.

Firewall will be deployed at each school locally, meaning the broadband service connects to a firewall that is located on an appliance or system on the school premises as either discrete technology or a component of another system.

Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.

The firewall should be checked XX (and recorded) to ensure that a high level of security is maintained, and there is effective protection from external threats.

Any compromise of security through the firewall is recorded using an incident log and reported to the DPO. IT Support will react to security threats to find new ways of managing the firewall.

6. Malware Prevention

TAMAT understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites, or removable media controls.

IT support will ensure that all devices have secure malware protection and undergo regular malware scans in line with requirements. IT support will update malware protection on a XXX basis to ensure it is up to date and can react to changing threats. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

Filtering of websites, as detailed in the 'User privileges and passwords' section of the policy will ensure that access to website with known malware are blocked immediately and recorded.

TAMAT schools will use mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users. IT support will review the mail security technology on a termly basis to ensure it is up to date and effective.

Staff members are only permitted to download apps on any school-owned device from manufacturer approved stores and with prior approval from the IT Co-ordinator. Where apps are installed the IT Co-ordinator will keep up to date with any updates, ensuring staff are informed of when updates are ready and how to install them.

7. User Privileges and Passwords

TAMAT understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. pupils will have different access to data and the network than members of staff, whose access should also be roll based.

The XXX will clearly define what users have access to and hold a written record of that information.

Staff passwords will be changed as and when they are needed.

Multi factor authentication will be used where possible on accounts.

A master user password for each package should be kept by the Headteacher, IT Co-ordinator or other nominated member of staff in a secure manner.

A multi-user account should be created for visitors to the school (volunteers, outside agency) and access filtered in line with the school regulations. Usernames and passwords should where possible be input by the member of staff responsible for this.

Staff who leave the Trust will be deleted from software packages (including email) on the day they leave their employment.

8. Monitoring Usage

Each school should have an Acceptable Use Policy and an Online Safety Policy that outlines what and how software packages will be monitored.

Records should be kept of any staff or pupil who accesses inappropriate or malicious content. This information can be used as evidence of a not yet discovered breach of network security. It also may be used to ensure the school is protected and that all software is up to date.

9. Removable Media Controls

TAMAT understands that staff and pupils may need to access the school network from outside the school site. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware.

Laptops, mobile phones, and tables will be encrypted to ensure they are password protected. This will prevent unauthorised access of data should they be lost.

IT support will ensure that any manufacturer passwords will be changed from the default by choosing a set password, the member of staff receiving the device should be prompted to change the password at first login.

Staff will use devices as outlined in the Staff Code of Conduct.

The Wi-Fi network at the school will be password protected and only provided as required to others.

10. Backing Up Data

Data at each school will be backed up XX and recorded with the date. Backups are retained for XX before being deleted. Backups should (where possible) be stored in a fireproof safe or offsite in a secure location.

Each school must follow the NCSC's guidance on backing up data where necessary, including:

- Identifying what essential data needs to be backed up
- Storing backed up data in a separate location to the original data
- Consider using the Cloud to store backed up data
- Referring to the NCSC's Cloud Security Guidance
- Ensuring that backing up data is regularly practised

Where possible backups should be run overnight and completed before the beginning of the following day. Only authorised personnel will be able to access backups of the data at each school.

The backup strategy will be tested frequently, details of the testing will be recorded.

11. Avoiding Phishing Attacks

Staff members will be provided enough access that allows them to perform their jobs.

Staff who have access as master users to accounts will avoid browsing the web or checking emails whilst using the account. Designated important accounts will have two-factor authentication included.

The Headteacher will ensure that all staff, pupils, and members of the school community are aware of acceptable use of social media and the information they share about the school and themselves in accordance with the Acceptable Use and Staff Code of Conduct Policies.

12. User Training and Awareness

Staff and pupils should have training on how to use the network appropriately in accordance with the school policies. This training should include identifying irregular methods of communication to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact should such requests be received. These communications can come in all sorts of forms – email, telephone, text, or social media requests.

Staff and pupils should be made aware of who to inform should they suspect such a breach, and who they should inform if they suspect someone is using their password.

13. Cyber Security Incidents

Any member of the school community who discovers a cyber-security incident will report it immediately to the Headteacher and DPO of the Trust.

When an incident is raised the DPO will record the following information:

- Name of the individual who has raised the incident
- Description and date of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved e.g., school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident
- Where the incident needs to be reported to the relevant authorities e.g., the ICO or police

The Trust DPO will take the lead in investigating the incident along with allocated members of staff from the school and will be allocated the appropriate time and resources to conduct this. The DPO should ascertain very quickly the severity of the incident and determine if any personal data was involved or compromised, producing a report at the end of the investigation.

If the DPO determines that the severity of the breach is low, the incident will be managed in accordance with the following procedures:

- In event of an internal breach, the incident is recorded using an incident log, and by identifying the user and website or service they were trying to access
- The school will work with the DPO and IT support to provide an appropriate response to the attack, including any in-house changes
- Updated staff training will be organised following a breach
- Any further action which could be taken to recover lost or damaged data will be identified – this includes the physical recovery of data, as well as the use of back-ups.

If the security risk is high the DPO will establish what steps need to be taken to prevent further data loss, which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process
- Taking systems offline
- Retrieving any lost, stolen or otherwise unaccounted for data
- Restricting access to systems entirely or to a small group
- Backing up all existing data and storing it in a safe location
- Reviewing basic security, including changing passwords and login detail on electronic equipment
- Ensuring access to places where electronic or hard data is kept monitored and requires authorisation

If an offence is committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.

The DPO is required to report personal data breaches to the ICO if there is a likelihood of risk to people's rights and freedoms. If the DPO decides that risk is unlikely, the breach does not need to be reported, however will need to justify the decision, and document the breach.

The DPO will notify the ICO within 72 hours of becoming aware of a breach where it is likely to result in a risk to the rights and freedoms of individuals. UK GDPR recognises that it is not always possible to investigate a breach fully within 72 hours. The information required can be provided in phases, provided it is done without delay.

In line with UK GDPR the DPO must provide the following information to the ICO when reporting a data breach:

- A description of the nature of the breach, including where possible the categories and approximate number of individuals concerned
- Categories and number of personal data records concerned
- Name and contact details of the DPO
- A description of the likely consequences of the breach

- A description of the measures taken, or proposed measures to be taken to deal with the breach
- A description of the measures taken to mitigate any possible adverse effects where appropriate

Were a TAMAT school has been subject to online fraud, scams, or extortion the DPO will also report this using the Action Fraud website.

The DPO and IT Support will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the systems are safe to use.

TAMAT is aware that it must seek permission from the ESFA to pay any cyber-ransom demands in the event of a cyber-crime.

14. Consideration of Further Notification

The DPO will consider whether there are any legal, contractual, or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in data security.

The DPO will assess whether notification could help the individual(s) affected, and whether the individual(s) could act on the information provided to mitigate risks e.g., by cancelling a credit card, or changing a password. In line with the 'Data Security Breach Incidents' section of the policy if many people are affected, or there are very serious consequences the ICO will be informed.

The DPO will consider, as necessary, the need to notify any third parties such as the police, insurers, professional bodies, funders, trade unions, website and/or system owners, banks and/or credit card companies who can assist in helping or mitigating the impact on individuals.

15. Monitoring and Review

This policy will be reviewed annually by TAMAT Trust Board, with updates made where necessary.