PROSPER TOGETHER
MULTI ACADEMY TRUST

CYBER SECURITY POLICY

APPROVED BY:

ROLE ……CHIEF EXECUTIVE OFFICER……

DATED ……

DATE	PREPARED BY	REVIEW DATE
OCT 2023	S. TIMMINS	OCT 2025

Cyber Security Policy

Contents **Page**

Prosper Together Multi Academy Trust (the 'Trust') refers to all the Trust member schools and the central team.

1. Introduction

Prosper Together Multi Academy Trust (the 'Trust') is committed to ensuring the risks and impact of cybercrime are reduced.

Cyber security has been identified as a risk for the Trust and every staff member needs to contribute to the mitigation of this risk to ensure data security.

The Trust has in place a range of technical cyber security measures, but all staff also need to be vigilant and act to protect the Trust's IT systems and resources.

The Trust is seeking to develop a 'speak up' culture and encourages all staff to report any potential incidents or near misses to improve the Trusts cybercrime awareness and security procedures. The Trust understands that cybercrime can be difficult to detect, however if a staff member breaches this policy, does not follow the procedures set out in this policy, or fails to report an incident they may be subject to disciplinary action.

This policy should be read alongside other data, IT and security policies set by the Trust or individual school. This includes, but is not limited to:

- Data Protection Policy
- Anti-Fraud and Corruption Policy
- Acceptable Use Policy
- Home Working Policy
- Financial Policy and Financial Procedures
- Staff Code of Conduct

2. Purpose and Scope

The purpose of this document is to establish systems and controls to protect the Trust from cyber criminals and associated cyber security risks, as well as to set out an action plan should the Trust fall victim to cybercrime.

The Academy Trust Handbook states:

Academy trusts must be aware of the risk of cybercrime, put in place proportionate controls and take appropriate action where a cyber security incident has occurred.

This policy is relevant to all staff and applies to all Trust services and devices, including smartphones, any personal equipment that has been authorised to be used on Trust systems and home working.

3. Cyber Security and Cybercrime

<u>Cyber Security</u>

Cyber security's core function is to protect the **devices** that we use (smartphones, laptops, tablets and computers), and the **services** we access online and at work from theft or damage, preventing unauthorised access to the vast amounts of sensitive and personal

information that is stored. Cyber Security measures include both technical measures and the measures undertaken by individuals to prevent cybercrime.

Cybercrime

Cybercrime is a criminal activity carried out using computers or the internet. hacking, phishing, malware, viruses or ransom attacks.

Common incidents of cybercrime include:

- **Ransomware** - this is the most significant threat facing the UK and other users globally. The highest proportion of cyber-attacks reported to the Department for Education from the sector are ransomware attacks. Ransomware is a type of malware, typically introduced to a network through a sophisticated phishing or social engineering attack. When the malware is in the network the attacker will seek out critical and valuable forms of data, with the aim of exfiltrating this and then encrypting it. The attacker will then demand a ransom in exchange for decryption of the data. Recently this type of attack has evolved to the attacker threatening to publish the compromised data unless the victim pays the ransom demand. Common targeted data includes:
  - financial systems
  - personal identifiable data
  - intellectual property
  - student coursework
  - staff personal records
  - MIS/SIMS databases

  The Academy Trust Handbook states that Trusts must obtain permission from Education and Skills Funding Agency (ESFA) to pay any cyber ransom demands. The ESFA supports the National Crime Agency's recommendation not to encourage, endorse, or condone the payment of ransom demands. Payment of ransoms has no guarantee of restoring access or services and is likely to result in repeat incidents.

- **Insider threats** - this refers to the occurrence of an individual within an organisation who uses their authorised access for malicious activities or to cause harm or damage. It can include:
  - unauthorised disclosure of information
  - altering of assessment results
  - intentional or un-intentional alteration of personal and/or sensitive information
  - compromising safeguarding information
  - access to financial records and/or staff payroll details
  - launching attacks on the network of the school
  - commit fraud

  An insider threat can include pupils.

- **Phishing** – this is a form of social engineering attack aimed to trick the user into giving their credentials or identity information to an attacker.

  Normally delivered in email messages that look authentic, with corporate/official logos. Phishing emails often contain links to websites which will install malware without the user knowing or they will contain an attachment, which once downloaded or opened, will install the malware onto the system.

  They tend to ask for verification of personal information, such as account numbers, passwords or date of birth. This can result in stolen accounts, financial loss and identity theft.

- **Mandate Fraud** - this often occurs as a result of a compromised email account, typically due to a phishing attack. The fraud occurs when the attacker contacts the victim claiming to be from an organisation they would make regular payments to.

  The attacker sits on a compromised email account monitoring the traffic, waiting for the opportunity to change bank payment details on an invoice. The attacker will often set up forwarding rules on a compromised email account to intercept communication without being noticed.

Consequences

The following are all potential consequences of cyber-crime which could affect the organisation and/or individuals:

- Breach of confidentiality and data protection
- Regulatory breach
- Reputational damage
- Business interruption
- Structural and financial instability
- Cost

4. Cybercrime Prevention

Given the seriousness of the consequences noted above, it is important for the Trust to take preventative measures and for staff to follow the guidance within this policy.

The Trust has put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as governance processes and controls and guidance for staff.

Technical Solutions

The Trust has implemented the following technical measures to protect against cybercrime:

- Firewall
- Anti-virus software
- Anti-spam software
- Auto or real-time updates on our systems and applications
- URL filtering
- Secure data backup
- Deleting or disabling unused/unnecessary user accounts
- Deleting or disabling unused/unnecessary software
- Advising use of strong passwords
- Disabling auto-run features

Governance Solutions

The Trust will ensure that governance processes monitor the implementation of this policy and related policies and will:

- Identify all critical data that the Trust holds.
- Ensure that access controls linked to critical data are regularly reviewed and access is removed for individuals who do not require it.
- Ensure that strong passwords and multi-factor authentication (MFA) is applied to business-critical data systems.
- Maintain central and/or local back-up systems for critical data, implementing more than one back-up solution where possible and moving towards cloud-based systems where possible/viable.
- Schools will undertake at least an annual review of all devices still in use that are no longer supported by the manufacturer but are essential to the organisation to ensure that they are isolated from the internet.
- The Trust Board will regularly review risks relating to Fraud and corruption, including cybercrime.

People solutions – Controls and Guidance for Staff

All staff must follow the policies related to cybercrime and cyber security as listed in section 1 of this policy.

All staff will be provided with alerts and/or training when there is a change to the law, regulation or policy or where significant new threats are identified and in the event of an incident affecting the Trust/School or any third parties with whom we share data.

All staff must:

- Choose strong passwords - the Network Manager advises that a strong password contains at least 8 characters including an uppercase, a lowercase, a numerical and a special character.
- Keep passwords secret.
- Never reuse a password.
- Never allow any other person to access the school's systems using your login details.
- Not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on computers, phones or network or the Trust IT systems.
- Not accept a remote access request by anyone but the Network Manager or a Unity IT Technician and only following a telephone conversation with the Network Manager, where this request is discussed.
- Implement Multi-Factor Authentication for systems where requested.
- Report any security breach, suspicious activity, or mistake made that may cause a cyber security breach, to **Irene Hand, Network Manager** and the **IT Helpdesk** as soon as possible from the time of the discovery or occurrence. Quick action is critical to safeguard systems and data. A senior member of staff in the School/Trust should also be advised and the Cybersecurity Incident Plan (see section 5 below) should be implemented. If your concern relates to a data protection breach, the Data Protection Policy (Data Breach) must be followed.
- Only access work systems using computers or phones that the Trust owns. Staff may only connect personal devices to the **Guest Wi-Fi** provided.
- Not install software onto Trust computer or phone. All software requests should be made to the Headteacher and approved by the Network Manager.
- Avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using Trust equipment and/or networks.
- Not open unexpected emails that contain limited information and request for a link to be followed or a document to be downloaded. This may include requests from emails that contain addresses and/or logos of reputable organisations, such as other schools, the Local Authority and suppliers. If in doubt, please verify with a phone call using a contact number obtained independently from the email or raise an IT Helpdesk query to review the email communication.

All staff must not misuse IT systems. The Trust considers the following actions to be a misuse of its IT systems and resources:

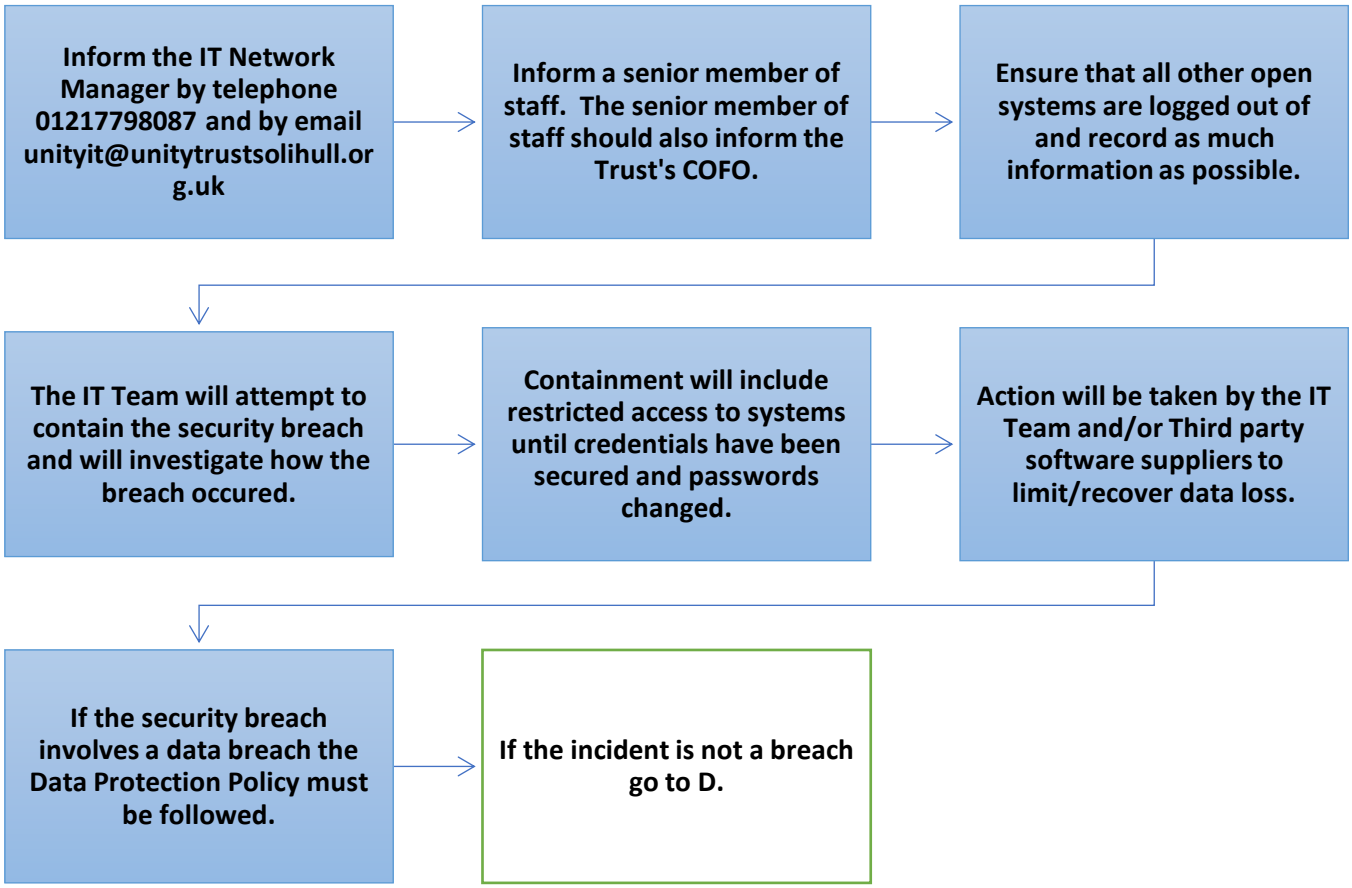
- Any malicious or illegal action carried out against the Trust or using the Trust's systems.
- Accessing inappropriate, adult or illegal content within Trust premises or using Trust equipment.
- Personal use of Trust's IT systems.

- Removing data or equipment from Trust premises or systems without permission, or in circumstances prohibited by this policy.
- Using Trust equipment in a way prohibited by this policy.
- Circumventing technical cybersecurity measures implemented by the Trust's IT team.
- Failing to report a mistake or suspected/actual cybersecurity breach.

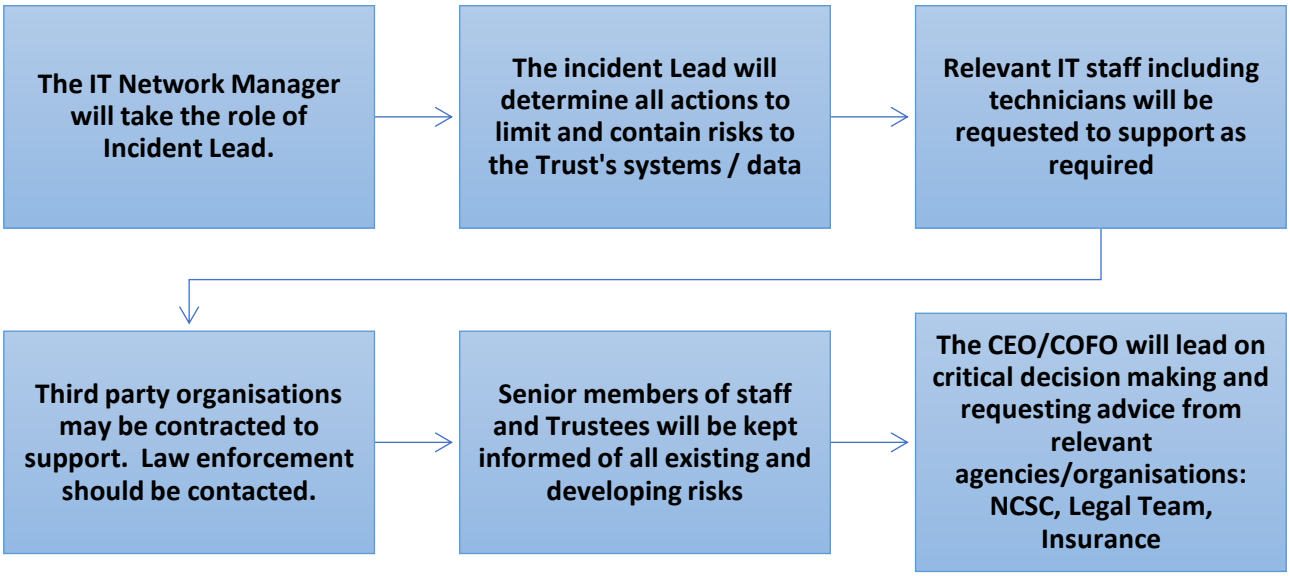
5. Cybercrime Incident Management Plan

The incident management plan consists of four main stages and should be implemented if a cybercrime incident is suspected and/or confirmed.

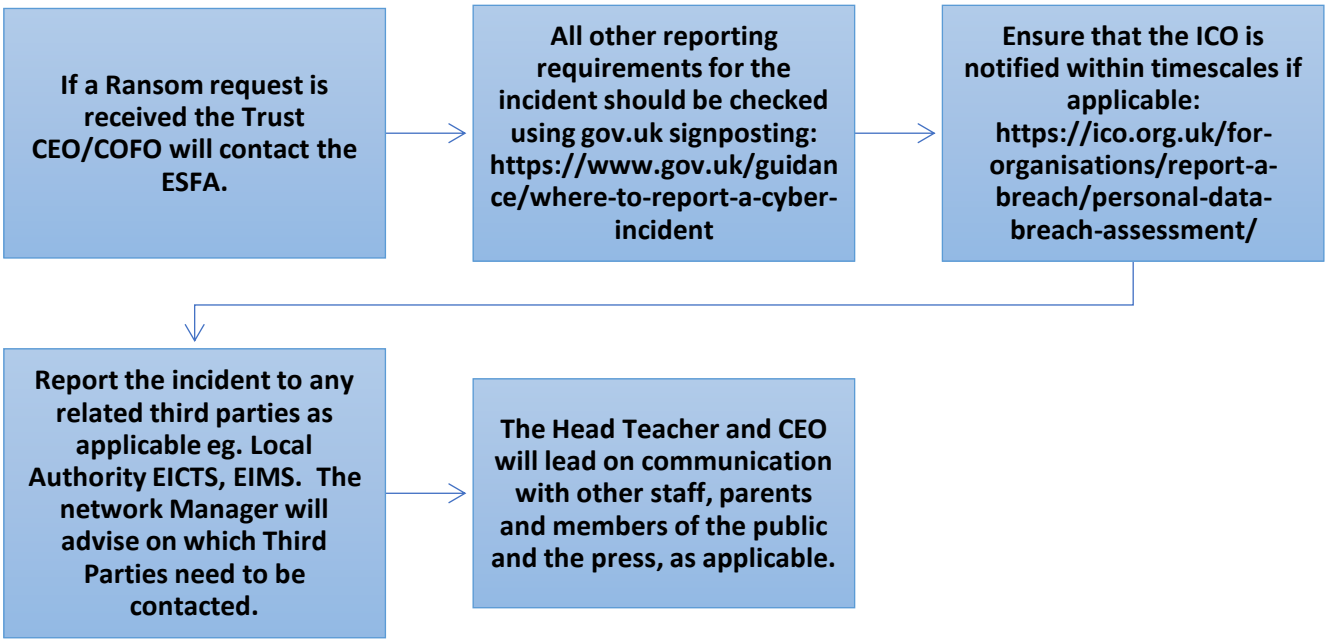
A. Containment and recovery: To investigate the breach, utilise appropriate staff to mitigate damage and where possible to recover any data lost.



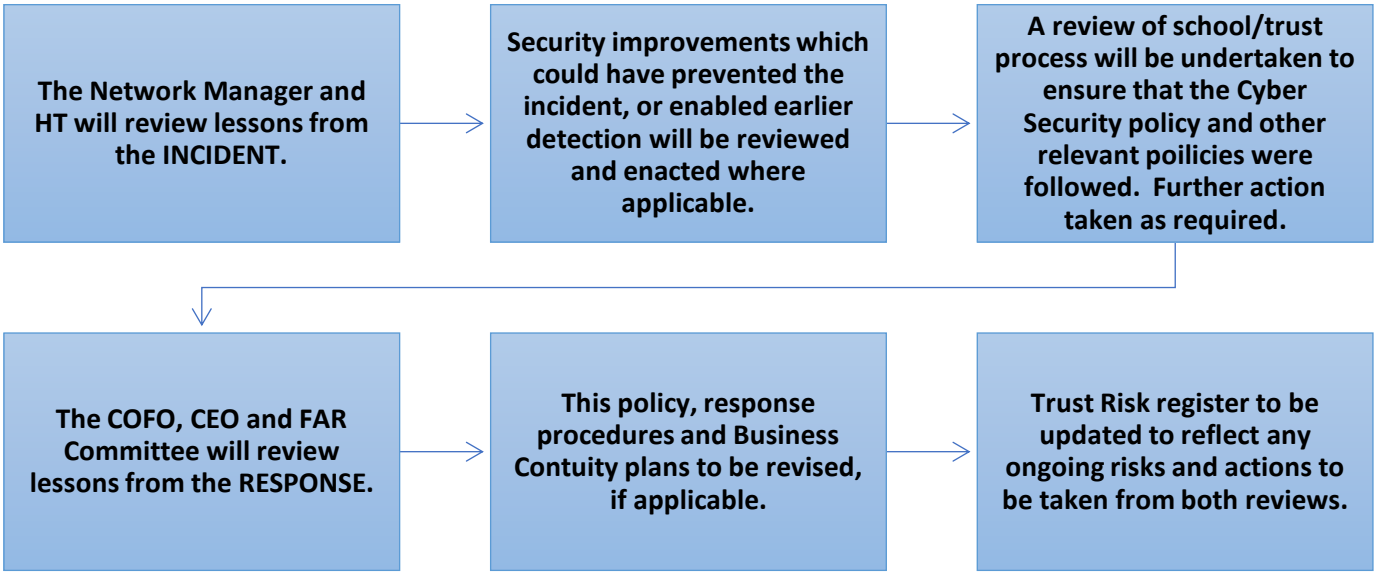
B. Assessment of the ongoing risk (if an incident is confirmed): To confirm what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed, and any consequences of the breach/attack identified.



C. Notification: To consider whether the cyber-attack needs to be reported and who to.



D. Evaluation and response: To evaluate future threats to data security and to consider any improvements that can be made.



6. Review

This policy will be reviewed every two years or earlier if there is a change to the law, regulation or policy or where significant new threats are identified and in the event of an incident affecting the Trust.

7. Sources of Further Information

National Cyber Security Centre (Schools): https://www.ncsc.gov.uk/section/education-skills/schools

Department for Education: https://www.gov.uk/government/publications/indicators-of-potential-fraud-learning-institutions/guide-on-cyber-crime-and-cyber-security-for-education-providers

Information Commissioners Office (Cyber Security): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/

Educational Resources: https://www.cyberfirstschools.co.uk