Cyber Security Policy 2025-26

Governor Responsible	
Committee Members	Glenn Tyreman, Head of Operations Ben Snedden, Network Manager
Author	Ben Snedden
Date of revision	Dec 2025
Date of next revision	Dec 2026

Introduction

This policy has been written to reduce the likelihood of a cyber security attack on Samuel Cody School and recognises such events can cause extreme financial and reputational damage to the school.

Scope

This policy applies to all staff, students, contractors, volunteers and visitors who have permanent or temporary access to and are users of the school computer and technology systems both on school premises or in the cloud. This includes all electronic hardware including but not limited to computers, tablets, memory devices, keyboards, mice and other input equipment at Samuel Cody School.

Brief and Purpose

Samuel Cody Schools cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

Samuel Cody School recognises the more technology is relied upon to collect, store and manage data, the more vulnerable we become to security breaches. Security breaches can come from internal sources e.g. a rogue or irate member of staff or external sources e.g. criminal gangs that use sophisticated methods to penetrate electronic data systems.

Regulatory

Samuel Cody School recognises the importance of complying with legislation and guidelines. All data is processed correctly and stored securely in accordance with the Data Protection Act 2018.

Samuel Cody School are aware data leaks and privacy violations can occur and this is covered by the Data Protection Policy.

Identified Risks

Targeted Attacks

High profile attacks against companies and Government agencies happen each and every year. The DfE could be penetrated one day and links used via third-party connectors (Wonde, Groupcall etc) into the schools MIS, Arbor are a

very real threat and the activity of these need to be monitored and audited for what they are actually doing.

Quishing

Fake QR codes. The use of using QR codes is not recommended throughout the school due to the increasing prevalence of fake QR codes.

Remote Access

Users do not have remote access to the school's onsite servers, data and equipment. Much of the school's data has been moved from onsite servers to the Microsoft 365 cloud environment negating the need for remote access.

The Network Manager does have remote access to various onsite servers and desktops to aid their role and provide remote support when not on site.

Personal Devices

Personal devices often have not had their updates and security patches applied, user access restrictions do not apply and are therefore recognised as an identified risk by Samuel Cody School.

The use of personal devices for all work undertaken for and on behalf of Samuel Cody School is for this very reason discouraged. The use of personal devices is covered by the Acceptable Use Policy.

The Acceptable Use Policy provides guidelines and advice on the acceptable use of electronic equipment for all staff, students, contractors, volunteers and visitors.

School devices are centrally managed and locked down through the use of security policies and user access restrictions meaning any breaches of computer and/or network security is limited and can quickly be isolated and shutdown.

Human Error

It is a common fact all humans make errors. Samuel Cody School have a medium-term plan to educate staff in recognising the common tactics used by criminals and criminal gangs to exploit this weakness.

Ransomware

Ransomware is designed to block access to the school's data by encrypting the data and demanding payment for the release of the school's data.

Samuel Cody School recognises the importance of protecting the school's data from ransomware and if a ransom is paid there are no guarantees the perpetrator/s have copied the data to be used or other purposes.

Denial of Service Attack (DoS or DDoS)

These attacks overload a school's website and network making them impossible to function normally.

The school's website is for informational purposes only and all information is already in the public domain will have no direct effect on the day-to-day function of the school and therefore is deemed of a low-level concern. If the schools website is subject to a Denial of Service Attack the school will liaise with the website host in the resolution of this attack and mitigating future attacks.

Phishing

Criminals and criminal gangs use scam emails, text messages or phone calls to trick potential victims into selecting links, revealing information, signing up to fake subscriptions and paying fake invoices.

The Network Manager has created a setup of rules that filter emails for known content and techniques used by criminals and criminal gangs. Emails that meet the criteria of the rules are quarantined and inspected for authenticity, if deemed to be genuine and safe will be released.

The content of scam emails are ever changing and the email rules are adjusted in response to these and when new information and techniques are known. All staff are aware they should forward any suspicious emails they receive to the Network Manager.

Account Takeovers and Reused Passwords

Account access is limited to restrict access to systems in the event of an account being hacked. Access is limited enough to not restrict staff and students to be able to complete their work in accordance with their roll and studies.

The Network Manager reviews current access requirements for all staff and students for all systems for all new starters, leavers and changing rolls. Guest accounts and access for contractors are monitored to ensure access is appropriate for requirements.

All staff are aware of not using the same passwords across different system logons and reusing passwords across different systems and using the same passwords for school and personal logons.

MFA/2FA (Multi-factor authentication/Two-factor authentication) is a short-to-medium-term plan to protect user logon accounts.

Wifi Networks

Wifi networks are visible to the outside world and can be connected to by persons simply being stood behind the fence of the school grounds or from properties nearby. Wifi networks can be hidden from view but can create issues for genuine school users if the device drops off the wifi network. It is an acceptable risk not to hide wifi networks due to wifi network passwords being a hidden secret and only known by the Network Manager and technical support staff.

The only exception is the guest wifi network. This is a logically separated network to the main school wifi networks and is available for guest access to the Internet.

Samuel Cody School operates multiple wifi networks to provide break points in the whole network connectivity chain. This provides resilience and continuity to areas of the network if one area is compromised enabling some functions of the school to still operate in the event of a cyber security breach.

Filtering of the Internet access is covered by the Internet Policy.

Data Backup

A daily online backup is taken every evening. This backups data resident on local servers in shared drives/folders and data stored in the Microsoft 365 cloud environment.

Accountability / Guidelines

Inappropriate use of the school computer systems and network will be in line with the Behaviour Policy and Acceptable Use Policy.

All staff will ensure all instances where human error, system malfunction and suspected cyber-attacks are reported to the Data Manager and the Network Manager immediately.

Safeguarding

Samuel Cody School recognizes the importance of student wellbeing. The schools Safeguarding Policy and Child Protection Policy are to be closely followed when a suspected cyber security breach has occurred.

Conclusion

Samuel Cody School recognises a cyber-security attack is not completely avoidable and are constantly undertaking measures and making improvements all the time to mitigate the chances of a cyber security attack and that prevention is better than cure.

Samuel Cody School recognises the benefits of using computer systems, the cloud and the Internet in education and is committed to providing a safe and supportive environment for our students. The guidelines outlined in this policy are in place to ensure safeguarding, transparency and maintain the academic and reputational integrity of the school.

All staff, students, contractors, volunteers and visitors must adhere to this policy when using the school computer systems, the cloud and the Internet.