Charlton Park Academy

Cyber Security Policy

Principal/Accounting Officer	Mark Dale-Emberton
Co-Chairs of Governors	Lynda Hage Graham Harknett
IT Technical Support	Muhammed Asad
Date approved	18.10.24
Date reviewed	October 2025
Date of next review and by whom	**Currently under review** CPA Governing Body

Introduction

A cyber security incident can have a major impact on any organisation for extended periods. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cyber Security Policy outlines guidelines and security provisions which are there to protect our systems, services and data in the event of a cyber attack.

Scope of Policy

This policy applies to all Charlton Park Academy staff, contractors, volunteers, and anyone else granted permanent or temporary access to school systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk Management

Compass Learning Partnership will include cyber security risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors three times per year.

Physical Security

CPA will ensure there are appropriate physical security and environmental controls protecting access to its IT systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, CPA will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform IT Department as soon as possible. Personal accounts should not be used for work purposes. CPA will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all CPA issued devices and data, users are required to:

- Lock devices that are left unattended.
- Update devices when prompted.
- Report lost or stolen equipment as soon as possible to the IT Department.
- Change all account passwords at once when a device is lost or stolen (and report immediately to the IT Department).
- Report a suspected threat or security weakness in CPA's systems to the IT Department.

Devices will be configured with the following security controls as a minimum:

- Password protection.
- Full disk encryption.
- Client firewalls.
- Anti-virus/malware software.
- Automatic security updates.
- Removal of unrequired and unsupported software.
- Autorun disabled.
- Minimal administrative accounts.

Data Security

CPA will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

CPA defines confidential data as:

- Personally identifiable information as defined by the Information Commissioner's Office.
- Special Category personal data as defined by the Information Commissioner's Office.
- Unpublished financial information.

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology:

- 3 versions of data
- 2 different types of media
- 1 copy offsite/offline

Sharing Files

CPA recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or if a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites.
- Wherever possible, keeping CPA's files on school systems.
- Not sending Trust files to personal accounts.
- Verifying the recipient of data prior to sending.
- Using file encryption where possible, sending passwords/keys via alternative communication channels.
- Alerting the IT Dept/Data Protection Officer to any breaches, malicious activity, or suspected scams.

Training

CPA recognises that it is not possible to maintain a high level of cyber security without appropriate staff training. It will integrate regular cyber security training into INSET days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

System Security
CPA's IT Department will build security principles into the design of IT services for the Academy:

- Security patching – network hardware, operating systems and software.
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them.
- Actively manage anti-virus systems.
- Actively manage and test backups.
- Regularly review and update security controls that are available with existing systems.
- Segregate wireless networks used for visitors' and staff personal devices from school systems.
- Review the security risk of new systems or projects.

Major Incident Response Plan
CPA will develop, maintain, and regularly test a Cyber Security Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers.
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again).
- Emergency plans for the school to function without access to systems or data.
- Alternative methods of communication, including copies of contact details.
- Emergency budgets and who can access them.
- Key agencies for support.

Maintaining Security
CPA understands that the financial cost of recovering from a major cyber security incident can far outweigh the ongoing investment in maintaining secure IT systems. CPA will budget appropriately to keep cyber-related risks to a minimum.