Charlton Park Academy
Information Security Policy

Date: October 2026
Review Date: October 2027

1. Purpose and Objectives

Charlton Park Academy is dedicated to ensuring the highest standards of information security. Under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the Academy is legally required to implement appropriate technical and organisational measures against unauthorised or unlawful processing, alteration, disclosure, accidental loss, destruction, or damage of personal data.

This policy defines the framework used by the Academy to:

- Protect against potential breaches of confidentiality;
- Ensure all information assets, school data, and IT facilities are protected against damage, loss, theft, or misuse;
- Support the Academy's Data Protection Policy by ensuring all personnel understand and comply with UK law;
- Foster a culture of cybersecurity awareness, defining individual responsibilities for handling data safely.

2. Scope

This policy applies to all written, spoken, and electronic information processed by or on behalf of Charlton Park Academy, regardless of the media or format. This includes network systems, cloud storage, paper records, emails, communication platforms, and verbal conversations.

The policy applies globally to all network users, including:

- Full-time, part-time, and temporary staff members;
- Governors and Trustees;
- Contractors, consultants, suppliers, and third-party partners;
- Volunteers and interns.

Compliance with this policy is mandatory. Any breach will be treated as a disciplinary matter and investigated under the Academy's Disciplinary Policy and Procedure, potentially resulting in disciplinary action up to and including summary dismissal for gross misconduct.

Note: This policy does not form part of any employee's contract of employment and may be amended at any time to remain compliant with changing legal obligations.

3. General Principles

3.1 Data Classification

All data processed on Academy systems or held in physical files must be classified into one of the following tiers, matching the definitions in the Data Protection Policy:

- Public (e.g., school brochures, public website content)
- Official / Internal (general operational data meant for staff eyes only)
- Personal Data (any information relating to an identifiable living individual)
- Special Category Data (highly sensitive personal data requiring enhanced protection, such as health records, safeguarding information, or biometrics)

Staff must consult their line manager if they are uncertain about the classification or required handling protocols of any dataset.

3.2 Access Control & System Authority

- **Principle of Least Privilege:** Access to systems and data is restricted to personnel with a legitimate, documented operational need to know.
- **Infrastructure Management:** All IT systems, hardware, and networks must be installed, maintained, repaired, and upgraded exclusively by the IT Department or vendors explicitly authorized by the Principal.
- **Accountability:** Overall responsibility for the security, integrity, and governance of IT systems rests with the Principal.

4. Physical Security & Workplace Environment

4.1 Desk and Display Security

- **Clear Desk Protocol:** Paper records containing personal or confidential information must not be left unattended on office desks, classroom tables, staffroom surfaces, or noticeboards. At the end of the working day, or when leaving a desk unoccupied, all such documents must be locked away in secure storage.
- **Screen Positioning:** Computer monitors and devices must be positioned to prevent **"shoulder surfing"** or viewing by unauthorized individuals passing by windows or glass panels.

4.2 Premises and Storage Protection

- **Secure Storage:** Physical locks, cabinets, and designated records storage rooms must be used and kept locked when not actively accessed.
- **Physical Audits:** The structural and physical security of buildings and storage facilities will be regularly reviewed by Premises staff to assess risks like burglary or vandalism. Staff must report any physical vulnerabilities to the Principal immediately.
- **Access Control:** The Academy maintains closed campus gates and an intercom verification system to prevent unauthorized entry.
- **Visitors:** All visitors must sign in at reception, wear an identification badge, and be accompanied by a staff member at all times. Visitors must never be left unattended in areas where confidential records could be accessed.
- **Surveillance:** CCTV cameras operate across the school premises for security monitoring, managed strictly by authorized Premises staff.

5. Computer, Device, and Network Security

5.1 Leadership & IT Management Responsibilities

The Principal, working in conjunction with the IT Department and Data Protection Officer (DPO), is responsible for:

- Assessing all IT infrastructure to ensure compliance with modern security baselines.
- Reviewing technical controls regularly and reporting outcomes to the Academy's Trustees.
- Ensuring staff receive regular IT security awareness training and updates regarding relevant legislation (e.g., UK GDPR, Computer Misuse Act 1990).
- Provisioning role-based access tokens and enforcing account security profiles.
- Ensuring that complete, automated, and secure backups of all critical systems are taken daily and stored in an encrypted, isolated offsite or cloud location.

5.2 User Device Rigour

- **Device Locking:** Staff must manually lock their screens (e.g., Windows Key + L) whenever walking away from an active terminal.
- **Automated Timeouts:** All Academy-issued computers, laptops, tablets, and smartphones are configured with a mandatory screen-lock timeout that activates after a short period of inactivity. Staff are prohibited from altering, extending, or disabling this timeout.
- **Shared Terminal Responsibility:** Staff must log out completely from shared terminals. Leaving a terminal logged in under your credentials makes you personally accountable for any actions taken on that device by another party.

5.3 Software and Asset Management

- **Installation Bans:** Staff are strictly prohibited from downloading, installing, or executing unauthorized software, browser extensions, or applications from external sources onto Academy devices. This includes instant messaging apps, games, media files, and screensavers.
- **Approval Pipeline:** Prior written approval must be obtained from the Principal before any new software tool can be evaluated or deployed.
- **Removable Media Restriction:** The use of unencrypted USB memory sticks, external hard drives, or legacy media disks is prohibited. Any approved physical media must be scanned by the IT department's anti-virus tools prior to file transfer. Cloud storage solutions must be approved by the Principal before use.

6. Access Control & Credential Integrity

6.1 Password Policy

Where legacy password login systems remain active, they must conform to the following **NCSC-aligned** standards:

- **Length & Complexity:** Passwords must be at least 12 characters long and include a mix of uppercase letters, lowercase letters, numbers, and symbols (or utilize a 3-random-words structure).
- **Uniqueness:** Passwords cannot match previously used iterations and must not contain easily guessable data (e.g., birthdays, sequential numbers, or names).
- **Confidentiality:** Credentials must never be shared, written down on sticky notes, or displayed openly. If passwords must be retained, they must be stored within an IT-approved secure corporate Password Manager.
- **Disciplinary Bounds:** Allowing another individual to use your login credentials, or logging into a device using another person's account, constitutes a severe breach of policy and will result in disciplinary action up to and including summary dismissal for gross misconduct.
- **Reset Protocol:** Forgotten passwords must be cleared by contacting the IT Service Desk. A new secure password must be set immediately upon account restoration.

6.2 Multi-Factor Authentication (MFA) & Biometrics

- **Mandatory MFA:** Multi-Factor Authentication (MFA) must be enabled on all staff accounts, remote portals, cloud environments, and core applications.
- **Biometrics:** Biometric sign-ins (e.g., facial recognition, fingerprint readers) may only be used on Academy devices if formally provisioned and approved by the IT Department.

7. Data Transmission and Communications

7.1 Electronic Transfers and Cloud Sharing

- **Encryption Mandate:** Any email or file transfer containing Personal Data or Special Category Data must be encrypted, password-protected, or shared via a secure, authenticated cloud link.
- **Address Verification:** Recipients' email addresses must be checked and confirmed manually before clicking 'Send'. Extra caution must be exercised with email "auto-complete" features to prevent misdirected data leaks.
- **Fax Discontinuation:** The use of fax machines for transmitting personal or confidential information is strictly prohibited due to intercept risks. Secure digital alternatives must be used.

7.2 Physical and Verbal Communications

- **Physical Mail:** Confidential physical documents must be sent via tracked, recorded delivery or a verified courier network.
- **Verbal Discretion:** Staff must maintain strict situational awareness and confidentiality when discussing school matters over the phone or in public spaces (e.g., trains, coffee shops, open staffrooms).
- **Data Transport:** If confidential data must temporarily leave the school site:
    - It must not be carried in transparent or unsealed bags;
    - It must never be left unattended in public places, public transit storage, or vehicle boots;
    - It must not be reviewed or read in public environments where it can be overseen.

8. Mobile Device Security & Remote Working

8.1 Device Protection

- **Storage Restrictions:** Local storage of personal or special category student/staff data on local device drives (laptops, tablets, mobiles) is prohibited without explicit written sign-off from the Principal. Data must reside on the Academy's secure cloud or network environments to ensure backup continuity.
- **BYOD (Bring Your Own Device):** Connecting personal mobile devices to the Academy’s corporate network or Wi-Fi is permitted only under strict compliance with the *BYOD Agreement*. The Principal reserves the right to disconnect or revoke access for any personal device at any time without prior notice.

8.2 Home Working Controls

- **Prior Authorization:** Confidential files or physical records must not be taken home without prior written permission from the Principal.
- **Home Environment Controls:** Staff authorized to work from home must ensure a secure environment where digital screens cannot be overlooked by family members or visitors, and physical documents are kept in locked storage when not in use.
- **Secure Disposal:** Confidential waste generated at home must not be discarded in domestic waste bins. It must either be shredded using a cross-cut shredder at home or brought back to the Academy premises for secure industrial shredding.

9. Incident Reporting & Threat Mitigation

9.1 Discovery and Notification

- **Duty to Report:** Every staff member has a mandatory obligation to report any actual, suspected, or potential data breach or security failure immediately to the Principal.
- **Technical Anomalies:** Technical bugs, malware indicators, hardware defects, or suspicious system behaviours must be reported directly to the IT Department.
- **Malware & Viruses:** If a virus, ransomware note, or phishing event is detected, it must be reported to IT immediately—even if system defences or anti-virus software appear to have successfully blocked or quarantined the threat.
- **Theft or Loss:** Any lost or stolen Academy asset (e.g., laptop, tablet, phone) or missing physical files must be reported immediately to the Principal so remote-wipe commands can be issued.

9.2 Breach Response Framework

- **No Self-Resolution:** Staff must never attempt to investigate or resolve a security incident or data breach independently. All remediation steps must be directed by the Principal and the IT Department.
- **DPO Escalation:** The Principal will immediately assess the severity of the reported incident. If the breach involves personal data, the Data Protection Officer (DPO) will be brought in to manage containment, risk logging, and legal notifications.
- **Regulatory Timelines:** If a data breach presents a risk to the rights and freedoms of individuals, the DPO must notify the Information Commissioner's Office (ICO) within 72 hours of the Academy becoming aware of it, in compliance with statutory UK GDPR requirements. All security incidents will be fully documented within the Academy's central risk register.

10. Policy Links & Framework Review

This policy operates alongside the following corporate policies:

- Data Protection Policy
- Data Breach / Incident Notification Policy
- Electronic Information and Communication Systems Policy
- Disciplinary Policy and Procedure

Review Cycle: This policy will be reviewed annually by the IT Management team, the Principal, and the DPO, or sooner in response to significant regulatory shifts, technological changes, or threat escalations.