STAMFORD PARK TRUST

CYBER SECURITY POLICY

DOCUMENT REFERENCE:	SPT/POL/000126/T
THIS POLICY APPLIES TO:	All staff and students
OWNER/AUTHOR:	COO/Head of IT
ESTABLISHMENT LEVEL:	Trust
APPROVING BODY:	Finance & Resources Committee
REVIEW CYCLE:	2 years
DATE APPROVED:	30th April 2025
LAST REVIEWED ON:	April 2025
NEXT REVIEW DUE BY:	April 2027
SUMMARY OF CHANGES:	Additions to sections 5, 9, 12 and 13
RELATED DOCUMENTS/POLICIES:	IT Acceptable Use Policy; Trust Safeguarding Policy
LEGAL FRAMEWORK/STATUTORY GUIDANCE:	

Contents

Registered Office: Ashton Sixth Form College, Darnton Road, Ashton-under-Lyne, Lancashire, OL6 9RL
T 0161 330 2330 **E** info@stamfordparktrust.ac.uk **www.stamfordparktrust.ac.uk**

Company registration number 11736886.

1. Introduction

Stamford Park Trust's Cyber Security Policy outlines the guidelines to protect against cyber-attack and provisions for preserving the security of our data and technology infrastructure.

Human errors, cyber-attacks and system malfunctions could cause great financial damage and may jeopardise the Trust's reputation. Cyber security is an important consideration when looking at due diligence and the expansion of the Trust when we take on new schools.

Educational institutions have come under increasing attention from cyber criminals utilising ransomware and phishing attacks to find weaknesses in schools & colleges. For this reason, we have implemented a number of security measures and have outlined both provisions in this policy and also refer all employees to other Trust Policies, such as the IT acceptable use policy.

2. Scope of the Policy

This policy applies to all our employees, contractors, students, pupils and anyone who has permanent or temporary access to our systems and hardware.

3. Personal device protection

When employees use their digital devices to access Trust emails or accounts, they introduce security risk to the data. We advise our employees to keep their personal devices secure and be aware of the IT Security Remote Working Policy. Staff must:

- Keep all devices password protected.
- Ensure antivirus software is kept up to date on personal devices.
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.

When new staff receive Trust-issued equipment they should review the Trust's Acceptable Use of ICT Policy, as it will contain key information relating to the safe and secure use of this equipment.

4. Company devices protection

Trust owned devices will be subject to regular automated anti-virus and security patches to ensure they are secure.

- Anti-virus signatures to be updated on a daily basis.
- OS security updates will be deployed on a weekly basis.

Theft or loss of a company device must be reported to the local IT Team as soon as possible.

Registered Office: Ashton Sixth Form College, Darnton Road, Ashton-under-Lyne, Lancashire, OL6 9RL
T 0161 330 2330 **E** info@stamfordparktrust.ac.uk **www.stamfordparktrust.ac.uk**

Company registration number 11736886.

5. Email attack mitigation

Emails often host phishing attacks, scams or malicious software. To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained.
- Be suspicious of clickbait titles.
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies in the structure and language of Emails.

If an employee isn't sure that an Email they received is safe, they should contact their local IT Team.

The Trust will run annual simulated phishing campaigns as part of its cyber training profile to educate staff on the dangers of such Email attacks.

6. Secure Data Transfer

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees seek the support of their local IT Team.
- Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Report scams, privacy breaches and hacking attempts to the local IT Team.
- Utilise secure email methods such as Egress or password protected archive files for the transport of sensitive data.

7. Password management

Password leaks can compromise the trust infrastructure or data. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. Further information regarding password security can be found in the Trust's Acceptable Use of ICT and Password Policies.

The Trust utilises a complex password policy to set the parameters for account passwords. Passwords must be at least 8 characters and contain a combination of uppercase, lowercase and special characters.

8. Education and training

Trust staff and students will receive annual training on cyber security and will be delivered via online training modules. All new staff will receive the training links as part of the induction process. The training will cover such aspects as:

Registered Office: Ashton Sixth Form College, Darnton Road, Ashton-under-Lyne, Lancashire, OL6 9RL
T 0161 330 2330 **E** info@stamfordparktrust.ac.uk **www.stamfordparktrust.ac.uk**

Company registration number 11736886.

- Phishing attacks
- Malware dangers
- Password security

9. Vulnerability Scanning

The trust will employ vulnerability scanning to check externally available systems for potential security holes. The systems will be scanned at the end of every month and subsequent report circulated to the central IT infrastructure team.

The IT department will run monthly internal scans on its network to look for internal security vulnerabilities using the PingCastle network tool. Each academy IT Team is responsible for ensuring the reported vulnerabilities at their location are acted on.

10. Multi Factor Authentication

Hackers attempt to force their way into systems by looking for weak username and password combinations to achieve a remote desktop connection. Once inside they can upload viruses or ransomware apps to encrypt data and shut down systems.

To mitigate against this the trust utilises Multi Factor Authentication for off-site or remote access to its services. Therefore, staff need two methods of authenticating in order to achieve a secure connection to the systems.

11. Patching Schedules

To close potential security holes, systems and applications need to have the latest security patches applied to them as soon as possible.

- Desktop systems will receive updates once a week, anti-virus signatures receive updates on a daily basis.
- More complex systems, such as servers and server applications are patched on a monthly basis.

12. Backup and restore regimes

Defences against cyber-attacks are important, but recovery from a potential breach is crucial so each area of the Trust has a robust backup regime including capacity for off-line data backup.

Off-line backup is when data is copied then stored in a location off the network, then should an organisation fall victim to a ransomware attack there will be a method of safe recovery. This is because ransomware will encrypt your live data, but can also encrypt backups that are part of the “live” network, thus rendering them useless for recovery.

Trust data is backed up onto disk on a daily basis and mirrored across the three sites. On a weekly basis data is backed up to encrypted tape which is then removed to an off-line status. In 2025 the Trust will implement a disaster recovery

Registered Office: Ashton Sixth Form College, Darnton Road, Ashton-under-Lyne, Lancashire, OL6 9RL
T 0161 330 2330 **E** info@stamfordparktrust.ac.uk **www.stamfordparktrust.ac.uk**

Company registration number 11736886.

centre at the Ashton Old Baths Data Centre with the aim of storing immutable backups from all the academies. This would then replace the tape backup solution as the off-site storage option.

Data and system restore are to be tested on a termly basis.

13. Security Certification and Audits

The trust will pursue cyber security certification as part of its IT security plan. The trust currently has self-certified Cyber Security Essentials and this is renewed on an annual basis. The Trust will have periodic internal audits on its Cyber Security environment as dictated by the Trust Audit Committee.

14. Safeguarding

Academies have a statutory duty to monitor their digital environment to identify any potential threats to students' welfare and wellbeing. The Trust's academies will have appropriate filtering and monitoring in place. Trust IT teams will work alongside safeguarding teams to ensure these systems are monitored and threats are reported appropriately. In the case of a specific allegation of misconduct, the safeguarding lead/investigating officer can authorise access to the specific content of transactions in order to investigate the allegation.

15. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action.

Deliberate and serious breach of this policy may lead to the Trust taking disciplinary measures in accordance with the Trust's disciplinary policy and procedure. The Trust accepts that IT – especially cloud-based systems for example as, but not limited to, cloud storage, applications and email systems. However, misuse of these facilities can have a negative impact upon employees' and volunteers' productivity and the reputation of the Trust.

Examples of deliberate or serious breaches of this policy and examples of misuse are, but not limited to:

- Knowingly disclose login information to an unauthorised third party
- Inappropriate disclosure of personal data
- Knowingly installing software on Trust devices that hasn't been approved by IT which leads to a breach.
- Allowing the use of Trust devices by unauthorised third parties

16. Reporting of incidents

Staff and students must report incidents or potential IT security breaches to the local IT Team as soon as possible. They must report the nature of the breach, the device used and any user account details so that the incident can be investigated fully.

- Longdendale High School – ithelpdesk@lhs.spt.ac.uk

Registered Office: Ashton Sixth Form College, Darnton Road, Ashton-under-Lyne, Lancashire, OL6 9RL
T 0161 330 2330 E info@stamfordparktrust.ac.uk www.stamfordparktrust.ac.uk

Company registration number 11736886.

- Fairfield High School for Girls – ithelpdesk@fairfieldhighschool.co.uk
- Rayner Stephens High School – ithelpdesk@rshs.spt.ac.uk
- Ashton Sixth Form College – ithelpdesk@asfc.spt.ac.uk
- John Haigh- Head of IT – j.a.haigh@spt.ac.uk

Registered Office: Ashton Sixth Form College, Darnton Road, Ashton-under-Lyne, Lancashire, OL6 9RL
T 0161 330 2330 **E** info@stamfordparktrust.ac.uk **www.stamfordparktrust.ac.uk**

Company registration number 11736886.