Cyber Security Policy

Approved by:	Trust Board
Last reviewed on:	13 May 2021
Next review due by:	Summer term 2022

1. Policy brief & purpose

Unity Schools Partnership's Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become, to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise our Trust's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy and also refer all employees to other Trust Policies.

2. Scope

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

3. Policy elements

Confidential data

Confidential data is secret and valuable. Common examples are:

- Information concerning staff, students, parents, governors and partners.
- Unpublished financial information and contractual data

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect personal and company devices.

When employees use their digital devices to access Trust emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and Trust-issued devices secure. They can do this if they:

- Keep all devices password protected.
- Ensure antivirus software is kept up to date.
- 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.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

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.

Keep emails safe.

Emails often host phishing attacks, scams or malicious software (e.g., trojans and worms.) 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 (e.g., “watch this video, it’s amazing.”)
- Be suspicious of clickbait titles (e.g., offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn’t sure that an email they received is safe, they should contact their local IT Technician or the Central IT Team.

Manage passwords properly.

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g., birthdays).
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person is not possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Change their passwords regularly, but at a minimum every six months.

Further information regarding password security can be found in the Trust’s Acceptable Use of ICT and Password Policies.

Transfer data securely

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 Technician or the Central IT Team for help.
- 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.

Our Local and Central IT Teams need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our Local or Central IT Team will investigate promptly, resolve the issue and send a Trust-wide alert when necessary.

Our Local and Central IT Teams are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to Local or Central IT Teams.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in company systems.
- Refrain from downloading suspicious, unauthorised or illegal software on their Trust equipment.
- Avoid accessing suspicious websites.

We also expect our employees to comply with our Acceptable Use of ICT and associated policies.

Our Local and Central IT Team will:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all employees as part of initial induction for new joiners and annually for existing staff.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy's provisions as other employees do.

Our company will have all physical and digital shields to protect information.

Remote employees

Remote employees must follow this policy's instructions as well. Since they will be accessing our Trust's information and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. Further information can be found in the Trust's Acceptable Use of ICT Policy.

We encourage them to seek advice from our Local and Central IT Teams.

4. 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.

In addition, all the Trust's phone, web-based, locally hosted systems and email related resources are provided for business purposes. Therefore, the Trust maintains the right to monitor all internet and local

network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use. However, see the Safeguarding section below.

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
- Storing data on insecure media such as removable media that leads to a breach.

Take security seriously.

Everyone should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and data. We can all contribute to this by being vigilant and keeping cyber security at the top of our minds.

5. Safeguarding

Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils' welfare and wellbeing. The Trust's schools have appropriate filtering and monitoring in place.

At Langer Primary Academy and in the Trust's secondary schools (including Churchill and Sir Bobby Robson) this monitoring is carried out by eSafe. eSafe combines intelligent detection software, expert human behaviour analysis and dynamic threat libraries to identify a range of safeguarding risks.

In schools using eSafe all school owned devices will be continuously monitored for safeguarding risks. If pupils and staff use a school owned device outside of school, the device will continue to be monitored when it is both online and offline. A Data Protection Impact Assessment (DPIA) has been completed for eSafe and an addendum added to the staff, pupil and volunteer privacy notices.

Schools not using eSafe regularly (at least half-termly) review the logs produced by their filters. Monitoring what is trapped by the filter allows schools to identify individuals using inappropriate search terms, so that they can be given advice/support, and to see any trends, which can be used to inform the school's curriculum/advice to staff, pupils and parents/carers.

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.

6. Reporting and Contact Information

Questions or reports relating to this policy should be addressed to:

Michael Vaughan – Head of IT – mvaughan@unitsp.co.uk

Pete McCarthy – Head of IT Operations – pmccarthy@unitysp.co.uk

Ben Shread – Head of IT Operations – bshread@unitysp.co.uk