Tonacliffe Primary School

Cyber Security Policy

September 2024

1. Developing and Reviewing this Policy

This Online Safety Policy has been developed by Ruth Noble (Computing Lead) and Debbie Wroe (School Business Manager).

Date policy created: January 2023

This Cyber Security Policy was approved by the Curriculum Committee on: 24th April 2023	
The implementation of this policy will be monitored by:	Joanne Heap (DSL) Ruth Noble (Computing and Online Safety Lead and Backup DSL) Debbie Wroe (School Business Manager)
The Cyber Security Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to cyber security, or incidents that have taken place. The next anticipated review date will be:	September 2025

This policy is linked to our:

- Child protection and safeguarding policy
- Data protection policy
- Acceptable use policy for staff, governors, and volunteers
- Acceptable use policy for visitors and contractors
- Staff code of conduct

1. Policy brief & purpose

Tonacliffe Primary School'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 school's reputation.

For this reason, we have implemented several 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 school 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, and governors.
- Unpublished financial information and contractual data.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 the school's emails or accounts, they introduce security risks to our data. We advise our employees to keep both their personal and school-issued devices secure.

They should do the following on school-issued devices and their personal devices if using these for work purposes:

- Keep all devices password protected (even if you only use your laptop for work, for example, this may be synched to your phone or tablet).
- Ensure antivirus software is kept up to date.
- Ensure they do not leave their devices exposed or unattended (if you leave the device unattended, at home or school, all devices need to be locked/put to sleep).
- Install security updates of browsers and systems monthly or as soon as updates are available. This includes ensuring your school-issued device is restarted regularly to ensure updates from our IT providers are completed.

● Log into school accounts and systems through secure and private networks only (Wi-Fi and VPN networks included).

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 school-issued equipment they should review the school'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 the email and names of people they received a message from to ensure they are legitimate.
● Look for inconsistencies or giveaways (e.g., grammar mistakes, capital letters, an excessive number of exclamation marks.)
● When accessing emails when not connected to the school WI-FI (such as at home, or on personal devices), staff have two-factor authentication set up.

If an employee isn't sure that an email they received is safe, they should contact the Convene 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.
Passwords for emails and computer log-ins are set by Convene IT and include randomised letters and numbers, which cannot be easily guessed.

For this reason, we advise our employees to:
● 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.
● Not keep combinations of identifiable information together. For example, do not keep their email address and password together or do not keep their passwords at the back of school lanyards.
● Exchange credentials only when necessary. When exchanging them in person is not possible, employees should use the phone instead of email, and only if they recognise the person they are talking to.
● Passwords for the computer log-ins, will be changed annually.

Transfer data securely.

Transferring data introduces a security risk.

Employees must:
● Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless necessary. When a mass transfer of such data is needed, we request employees seek the support of Convene IT 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 IT technicians, Convene IT needs 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 IT technicians will investigate promptly, resolve the issue, and contact the school if necessary. 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 Ruth Noble (Computing lead), Debbie Wroe (School Business Manager), and Convene IT.
● Report a perceived threat or possible security weakness in company systems to Ruth Noble (Computing Lead) and Convene IT.
● Downloading of software is disabled on staff and pupil accounts without the use of an elevated user account which is entered by Convene IT.
● Avoid accessing suspicious websites. We also expect our employees to comply with our Acceptable Use of ICT and associated policies.
● Log out of emails every time a session is finished.
● Not use apps on phones such as Mail or Outlook to access work emails (these have now been blocked).

Convene IT, our IT technicians, will:
● Install firewalls, anti-malware software, and access authentication systems.
● Investigate security breaches thoroughly.
● Follow this policy's provisions as other employees do.

As an additional measure, we have implemented the Police CyberAlarm tool on our school system. This monitoring solution will help to detect and provide regular reports of any suspicious cyber activity targeting the school IP address. Any reports and monthly information from Police CyberAlarm will be received by Ruth Noble (Computing Lead) and the IT admin address accessed by Convene IT.

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

Remote working.

When working remotely, staff must follow this policy's instructions as well.

Since they will be accessing our school'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.

4. Response to cyber attack

If staff perceive a threat or possible security weakness/breach, they must contact Ruth Noble (Computing Lead) and Convene IT. Within our SLA with Convene IT, we may raise concerns with them over the weekend if security had been compromised.

Convene IT's solution to a Ransomware or Disaster Recovery incident would be:

1. Assess the impact of the incident – has it targeted servers, file shares as well as workstations and isolate them from the network.
2. Recover your server from the latest available backup either via the backup drives that are swapped daily or from the nightly cloud backup, to existing or loaned hardware as required.
3. Use the server/ bootable media to wipe and reinstall impacted workstations with a fresh installation of Windows and key applications.
4. Ensure users can log on to access their files and the internet.
5. Monitor the network activity for the next week to ensure the incident has been remediated.

5. 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 breaches of this policy may lead to the school taking disciplinary measures in accordance with the school's disciplinary policy and procedure.
All the school's phone, web-based, locally hosted systems and email-related resources are provided for business purposes.
Therefore, the school 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 are not limited to:

- Knowingly disclose login information to an unauthorised third party
- Inappropriate disclosure of personal data
- Knowingly installing software on school devices that hasn't been approved by IT which leads to a breach.
- Allowing the use of school devices by unauthorised third parties.
- Using school devices for anything other than work-related matters.

• 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.

6. Safeguarding

Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils' welfare and well-being.
We have appropriate filtering and monitoring in place. The monitoring is carried out by Smoothwall. Smoothwall runs on all school-owned devices and is 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. If an incident arises, Smoothwall will contact the necessary staff with the required information.

For any concerns related to staff accounts, Ruth Noble (Computing Lead, Back-Up DSL) and Joanne Heap (Headteacher, DSL) will be contacted.
For any concerns related to pupil accounts, Ruth Noble (Computing Lead, Back-Up DSL), Joanne Heap (Headteacher, DSL), Charlotte Clutterbuck (Acting Deputy Headteacher, Back-Up DSL) and Amy Griffiths (SENCO, Back-Up DSL).

Through our internet provider, we use Fortinet to filter. This is rolled out for staff and pupils. Pupils have a higher level of protection than staff.

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, Ruth Noble (Computing Lead, Back-Up DSL) and Joanne Heap (Headteacher, DSL) can authorise access to the specific content of transactions in order to investigate the allegation.