** Mill Lane Community Primary School &**

 **The Windmill Community Nursery**

**Growing, Thriving, Flying**

 **Cybersecurity Policy**

This policy applies to Mill Lane Community Primary School and its extended services, as well as the Windmill Community Nursery. It applies to all our staff, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

**Policy Brief and Purpose**

This 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 a number of security measures. We have also prepared instructions that will help mitigate security risks. We have outlined both provisions in this policy and also refer staff to other school policies.

**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* Unpublished financial information and contractual data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 school emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and school-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 school accounts and systems through secure and private networks only

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

**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 emails 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 our IT technician from Turn It On

**Password Management**

Password leaks are dangerous since they can compromise the 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 staff to:

* Choose passwords with at least 8 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 staff 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, staff 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.

**Transfer Data Securely**

Transferring data introduces security risk. Staff must:

* Avoid transferring sensitive data e.g. employee records to other accounts or devices unless absolutely necessary. When mass transfer of such data is needed, we request staff seek the support of the IT technician for help.
* Share confidential data over the school network / system and not over public Wi-Fi or private connection.
* Ensure that the recipients of data are properly authorised people or organisations and have adequate security policies.
* Report scams, privacy breaches and hacking attempts.

The school needs to know about scams, breaches and malware so that we can better protect our infrastructure. For this reason, we advise staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to Turn It On and the school’s bursar.

**Additional Measures**

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

* Turn off their screens and lock their devices when leaving their desks.
* Report stolen or damaged equipment as soon as possible.
* Change all account passwords at once when a device is stolen.
* Report a perceived threat or possible security weakness in the school’s systems.
* Refrain from downloading suspicious, unauthorised or illegal software on their school equipment.
* Avoid accessing suspicious websites.

Our IT support team will:

* Instal firewalls, anti-malware software and access authentication systems.
* Arrange for security training for all employees annually.
* 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 school will have all physical and digital shields to protect information.

**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 school taking disciplinary measures in accordance with the school’s disciplinary policy and procedure. The school 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 school.

In addition, 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 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 the IT support team which leads to a breach.
* Allowing the use of school 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.

**Safeguarding**

Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils’ welfare and wellbeing. The school has appropriate filtering and monitoring in place.

The School regularly (weekly) reviews the logs produced by their filters. Monitoring what is trapped by the filter allows the school 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.