**Windmill Pre-School – Cyber Security Policy**

As an educational setting it is important that we protect the sensitive information about the setting and the children we care for from accidental damage and online criminals.

Early Years education and childcare settings, like most other work environments, are increasingly reliant on technology. Smartphones, computers, laptops and tablets are a fundamental part of modern life Early Years practitioners. Good cyber security means protecting and safeguarding, the personal or sensitive information we hold on our children and their families. Early Years legislation and advice and the Data Protection Act requires us as a setting, to hold confidential information and records about staff and children securely, and ensure these can only be accessed by those who have a right or professional need to see them (either physically or digitally/online).

We will take the following steps to ensure and maintain cyber security

**Back up important information**

We will back up our most important information including sensitive information about the children in our care, their families, staff records, family contact details in an emergency, and other highly personal information. We will also back up email, fee payments, banking and invoices. Which we are legally required to safeguard. We will make a backup copy on a USB stick, an external hard drive, or 'in the cloud'. This will be kept away from the premises in case of an accident, fire/flood/theft or other loss.

**Using passwords to control access to our computer and information**

Passwords are an effective way to ensure that unauthorised persons do not have access to email accounts, data etc.

Email account should have a strong password to avoid it being hacked.

All passwords should be written on a piece of paper and kept somewhere safe and away from the computer.

It is safe for passwords to be saved in the browser if asked to do so.

If more than one person used the computer you should ideally use different log ins

**Communicating safely with our families (including social media)**

When we send out newsletters, social media posts, or any other communications that include photos or details of children in our care, we must ensure that we control who can access these. For example, you should password protect newsletters so only families who have been given the password can open them. You should also check the privacy settings across any social media accounts you use, so that only the child's carers have access.

**Turn on antivirus product**

You should always use antivirus software on the laptops and other computers in your setting. It's often included for free, so it's just a matter of turning it on, and keeping it up to date. Most modern smartphones and tablets don't need [antivirus software](https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product), provided you only install apps and software from official stores such as Google Play and Apple's App Store.

**Keep all your IT devices up to date**

Updates include protection from viruses and other kinds of malware, and will often include improvements and new features. Applying software updates is one of the most important things you can do to protect your devices. Update all apps and your device's operating system when you're prompted. You can also turn on 'automatic updates' in your device's settings, if available. This will mean you do not have to remember to apply updates.

**Dealing with suspicious messages (phishing attacks)**

'Phishing' emails are scam messages that try to convince you to click on links to dodgy websites, or to download dangerous attachments. The websites might try and trick you into giving sensitive information away (such as bank details), and the attachments can contain computer viruses that will infect your machine.

Many phishing emails are currently [preying on fears of COVID-19](https://www.bbc.co.uk/news/technology-51838468), but criminals can also use other methods to trick you, such as sending text (SMS) messages, or by phone. However, the term 'phishing' is mainly used to describe scams that arrive by **email**.

**Help your staff to spot unusual requests**

We should ensure that staff know what to do with unusual emails or phone calls, and where to get help? Is someone *impersonating* an important individual (a parent, manager, or member of the local authority) and how they would be challenged. We need to encourage and support staff to question suspicious or just unusual requests, even if they appear to be from important individuals. Having the confidence to ask ‘is this genuine?’ can be the difference between staying safe, or a costly mishap.

**Reporting suspicious messages**

If we receive a message from an organisation or person that doesn't normally contact us, or if something just doesn't feel right, we will report it. It will be helping the NCSC to reduce criminal activity, and in the process, prevent others from becoming victims.

* A suspicious email, should be forwarded to the NCSC's [Suspicious Email Reporting Service](https://www.ncsc.gov.uk/information/report-suspicious-emails) at **report@phishing.gov.uk**.
* If we received a suspicious **text message**, forward it to **7726**. This is a free-of-charge service for reporting spam to your network operator.

**What to do if you've already responded**

If you've already responded to a suspicious message, here's what to do:

* If you think any of your accounts (including email accounts) have already been hacked, refer to our [guidance on recovering a hacked account](https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account) (which includes what to look out for).
* If you’ve been tricked into providing your banking details, contact your bank and let them know.
* If you've given out your password, you should [change the passwords](https://www.ncsc.gov.uk/cyberaware#action-1) on any of your accounts which use the same password.
* If you've lost money, tell your bank and report it as a crime to [Action Fraud](https://www.actionfraud.police.uk/), the reporting centre for cyber crime for those in England, Wales and Northern Ireland. You can contact them on 0300 123 2040. In Scotland, contact the police by dialling 101 or via the [Police Scotland website](https://www.scotland.police.uk/contact-us/report-fraud).

**This policy was adopted on 31st August 2021 and amended on 8th September 2022**

**Bryony Smith - Chair of Windmill Pre-School Management Committee**

**……………………………………….**

**Claire Baker –Manager of Windmill Pre-School**

**……………………………………….**