Cyber Security Policy

At St Catherine's Independent Nursery we recognise that the key to keeping our nursery cyber secure is through effective staff training so that everyone is aware of the actions they should take to protect our systems from threat.

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity, e.g. scam emails. All staff are reminded to follow our procedures including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure.

To prevent any attempts of a data breach (i.e. when our information is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with, we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the National Cyber Security Centre (NCSC) Suspicious email reporting service at report@phishing.gov.uk.

Procedures

Passwords

We will:

- Create strong and memorable passwords for important accounts, such as by combining three random words. We will avoid using predictable passwords, such as dates, family and pet names. Passwords will not be reused
- All staff must use a separate password for work and personal accounts
- Passwords will be stored using password managers with end-to-end encryption
- We use multi-factor authorisation (MFA) to log in where appropriate, e.g. banking websites.

Security

- We train staff to recognise the techniques that phishers use in emails, as well as recognising spam and other harmful content
- Staff must report suspicious messages or links to management
- We carry out regular software updates and regularly check our back-ups
- Staff always lock devices when not in use
- We use PIN or password ID on portable devices
- We do not install any software that has not been cleared for use by the manager onto our computers or systems
- Unknown USBs or external devices will not be used on our systems.

Reporting

- Staff are encouraged to ask for further guidance or support from their manager when something feels suspicious or unusual
- Staff are encouraged to flag concerns and must report attacks as soon as possible.

System access

- We use a separate 'guest' WiFi for visitors to limit access to the office network
- We regularly review system access
- Accounts are removed immediately when a staff member has left employment.
- We limit access for temporary workers
- Staff follow sign-in/out protocols
- No staff member has access to nursery devices outside working hours.

Actions in the event of a cyber attack

- Manager will be informed immediately of any actual or suspected security breach
- We will contain the breach, isolate affected devices and disable compromised accounts
- We will avoid deleting anything that could serve as evidence
- We will keep a log of actions taken and notify the Information Commissioner's Office (ICO) if personal data is at risk (https://ico.org.uk/for-organisations/report-a-breach/)
- We will seek advice and guidance from the National Cyber Security Centre (NCSC) (https://report.ncsc.gov.uk/)
- We will communicate clearly with staff and stakeholders to explain what's happened, what we're doing and how it affects families and staff
- Following an actual or suspected attack, we will review our systems to identify what occurred, what was compromised and what changes are needed.

This policy was adopted on	Signed on behalf of the nursery	Date for review
03/03/2026	*H Brockliss*	03/03/2027