Cyber Security Policy

This policy should be read alongside the nursery's Data Protection and Confidentiality Policy, Acceptable Internet Use Policy and Online Safety Policy.

At St Bernards Day Nursery, we recognise the importance of protecting the personal and sensitive information we hold about children, families and staff. We take appropriate steps to protect our devices, systems and information from unauthorised access, loss, misuse and cyber threats.

Cyber criminals can target any organisation, including early years settings. Staff are therefore expected to follow nursery procedures for secure passwords, safe use of devices, data protection and the reporting of suspicious activity.

Suspicious Emails, Messages and Links

Staff must not open, reply to, download attachments from or follow links in messages that appear suspicious or unexpected. This may include messages about resetting passwords, compensation, scanning devices, missed deliveries or other requests for personal or account information.

Any suspicious message, link or activity must be reported to the Nursery Manager as soon as possible. Where appropriate, suspicious emails may also be reported to the National Cyber Security Centre (NCSC).

Passwords and Account Security

- Strong and memorable passwords will be used for important nursery accounts.
- Predictable passwords, such as dates, family names or pet names, should not be used.
- Passwords must not be reused across nursery accounts.
- Staff must use separate passwords for work and personal accounts.
- Multi-factor authentication (MFA) will be used where appropriate and available.
- Passwords and account details must not be shared with unauthorised persons.

Device and System Security

- Software and devices will be kept up to date where appropriate.
- Nursery information will be backed up appropriately, and backups will be checked.
- Devices must be locked when they are not in use.
- Portable devices will be protected by an appropriate PIN, password, fingerprint or Face ID.
- Software must not be installed on nursery devices without the approval of the Nursery Manager.
- Unknown USB drives or external devices must not be connected to nursery systems.
- Nursery devices must be used in accordance with the setting's policies and procedures.

System Access

- Access to nursery systems will be limited to those who require it for their role.
- System access will be reviewed regularly.
- Accounts will be removed promptly when a member of staff leaves employment.
- Access for temporary workers will be limited as appropriate.
- Staff must follow nursery sign-in and sign-out procedures.
- Visitors should not be given access to secure nursery systems or confidential information.

Reporting Concerns

Staff must report any actual or suspected cyber security concern, unusual activity, lost or compromised device, suspicious message, or possible unauthorised access to the Nursery Manager immediately. Staff should seek guidance whenever something appears suspicious or unusual.

Action in the Event of a Cyber Attack or Data Breach

- The Nursery Manager will be informed immediately of any actual or suspected security breach.
- Where possible, affected devices will be isolated and compromised accounts secured or disabled.
- Information that may be required as evidence will not be unnecessarily deleted.
- A record will be kept of the incident and the actions taken.

- Where personal data may be at risk, the nursery will follow its data protection procedures and consider whether the incident must be reported to the Information Commissioner's Office (ICO).
- Advice and guidance will be sought from the National Cyber Security Centre (NCSC) where appropriate.
- Relevant staff, families and other stakeholders will be informed where necessary and appropriate.
- Following an incident, the nursery will review what happened, what information or systems were affected and whether any changes are required to reduce future risk.

Monitoring and Review

The Nursery Manager is responsible for ensuring this policy is implemented. The policy will be reviewed regularly and following any significant cyber security incident or relevant change to nursery systems or procedures.