Cyber Security Policy

Purpose

This policy outlines the cybersecurity measures to protect the sensitive data of Pavilion Pre School (Aigburth) CIO, including that of its staff, children, and parents, against unauthorised access, cyber threats, and data breaches. As a not-for-profit charity, we are committed to safeguarding the privacy and security of personal data in line with the General Data Protection Regulation (GDPR), Data Protection Act 2018, and other applicable legislation.

Scope

This policy applies to all staff, volunteers, trustees, and any third parties who may have access to the Charity's digital infrastructure, systems, or data. This includes the preschool's website, emails, digital records, databases, devices (e.g., laptops, tablets, and phones), and any other electronic systems.

3. Key Cybersecurity Responsibilities

- Staff and Volunteers: All staff and volunteers are responsible for adhering to this cybersecurity policy and implementing safe practices when handling sensitive data.

- Data Protection Officer (DPO): The Charity's DPO (or designated responsible individual) is accountable for overseeing compliance with data protection regulations, managing data breaches, and ensuring cybersecurity policies are followed.

- IT Support Services: Any external or internal IT support services must comply with this policy and ensure that secure systems are maintained, such as antivirus software, firewalls, and regular backups.

Cyber Security Policy

Access Control

- User Access Management:

Access to all digital systems and data will be limited to authorized users only. User accounts will be created based on role and need-to-know principles.

    - Staff and volunteers will be provided with unique usernames and passwords to access systems.
    - Shared accounts are prohibited.
    - User accounts will be disabled or removed when an employee or volunteer leaves the Preschool.

- Password Security:

    - Strong passwords (at least 8 characters, combining letters, numbers, and special characters) must be used.
    - Passwords must not be shared, written down, or stored insecurely.
    - Passwords should be changed regularly (at least every 90 days).

- Two Factor Authentication or Multi-Factor Authentication (MFA): Wherever possible, TFA or MFA will be enabled to add an extra layer of security to sensitive systems and accounts.

5. Data Protection and Confidentiality

- Sensitive Data Handling: Personal data, including that of children, parents, and staff, must be stored securely. Paper-based records should be stored in locked cabinets, and digital records should be encrypted and access-controlled.

- Data Minimization: Only the data that is necessary for specific purposes should be collected and stored. Data should not be kept longer than needed and should be regularly reviewed for retention and deletion.

- Data Sharing: Personal data must not be shared with unauthorized parties. If data needs to be shared externally (e.g., with a partner organisation), it must be protected through secure means (e.g., encrypted emails or secure file transfer services).

Cybersecurity Awareness and Training

- Training Programs: All staff, volunteers, and trustees must undergo regular cybersecurity training to recognise phishing attacks, secure sensitive data, and understand safe online practices.

- Phishing Awareness: Staff should be educated on identifying suspicious emails or requests for personal information (phishing). They should report any suspected phishing emails to the DPO immediately.

IT Systems and Infrastructure Security

- Antivirus and Anti-Malware: All devices used by the Charity (computers, tablets, smartphones, etc.) should have up-to-date antivirus and anti-malware software installed.

- Software Updates and Patch Management: The Charity's software, operating systems, and applications should be regularly updated to protect against known vulnerabilities.

- Firewalls and Network Security: Firewalls should be implemented to block unauthorized access to the Charity's internal network, and network traffic should be monitored for suspicious activity.

Cyber Security Policy

Incident Response and Reporting

- Cybersecurity Incident Reporting: Any staff member or volunteer who identifies a cybersecurity threat or data breach must immediately report it to the DPO or designated point of contact. This includes any suspected phishing attempts, malware infections, or unauthorised access attempts.

- Data Breach Response: In the event of a data breach, the Charity will follow the steps outlined in its Data Breach Policy:

    - Notify affected individuals without undue delay if their personal data is compromised.

    - Report the breach to the Information Commissioner's Office (ICO) within 72 hours, if required by GDPR.

Mobile Device Security

- Mobile Device Management: All mobile devices that access the Charity's data (e.g., smartphones, tablets) must be secured with passwords or PINs. These devices must be encrypted, and sensitive data must not be stored locally on these devices unless necessary.

- Remote Work Security: If staff or volunteers work remotely, secure VPN (Virtual Private Network) connections must be used to access the Charity's systems and networks.

Cyber Security Policy

Backup and Recovery

- Data Backup: Regular backups of critical data should be taken and stored securely. These backups must be tested periodically to ensure they can be restored in the event of a system failure or data loss.

- Disaster Recovery Plan: A disaster recovery plan should be in place, detailing the steps to restore data and IT systems in the event of a breach, cyberattack, or other disruptive incidents.

Third-Party Vendors

- Third-Party Cybersecurity: The Charity must ensure that any third-party vendors or service providers that handle sensitive data comply with cybersecurity standards. Data processing agreements must be signed, and the vendor's security measures should be assessed regularly.

Policy Review and Updates

This policy will be reviewed annually or in response to any significant cybersecurity incidents or changes in relevant legislation (such as updates to GDPR or cybersecurity regulations). All staff, volunteers, and trustees will be informed of any changes to this policy.

This policy was adopted in May 2025/
It will be reviewed annually or as and when required.
Last updated: 30.09.26

Signed by Chair of Trustees:

Signed by Operations Manager: