St John Lloyd RC Primary School

Cyber Security Policy 2026/27

Policy Statement

St John Lloyd RC Primary School is committed to protecting its digital systems, devices, networks, data and users from cyber threats. The school recognises that cyber security is essential to safeguarding learners, staff, governors and school information and forms an integral part of our safeguarding responsibilities.

This policy establishes the expectations and procedures required to maintain a secure digital environment and support the safe use of technology across the school.

Aims

The aims of this policy are to:

- Protect personal and sensitive information held by the school.
- Ensure the confidentiality, integrity and availability of school systems and data.
- Reduce the risk of cyber attacks including phishing, malware, ransomware and data breaches.
- Promote safe and responsible use of digital technology.
- Meet legal and statutory obligations, including UK GDPR and Data Protection legislation.
- Support the Welsh Government's Digital Competence Framework and Hwb guidance.

Scope

This policy applies to:

- All staff
- Governors
- Volunteers
- Contractors
- Trainees
- Visitors using school systems
- Learners when accessing school technology

The policy covers all school-owned devices and any personal devices authorised for work-related use.

Roles and Responsibilities

Headteacher

The Headteacher will:

- Ensure appropriate cyber security measures are implemented.
- Ensure staff receive cyber security training.
- Report significant cyber incidents to the Local Authority and relevant agencies.
- Ensure compliance with this policy.

Governing Body

Governors will:

- Monitor compliance with this policy.
- Support the allocation of appropriate resources for cyber security.
- Review cyber security risks as part of school risk management.

Staff

All staff must:

- Follow security procedures at all times.
- Complete required Hwb and cyber security training.
- Use strong passwords and keep them confidential.
- Immediately report suspected cyber incidents.
- Ensure personal data is handled securely.

Learners

Learners must:

- Follow the school's Acceptable Use Agreement.
- Keep passwords private.
- Report anything suspicious or concerning online.
- Use school technology responsibly.

Password Security

All users must:

- Use strong passwords containing at least three random words or a combination of letters, numbers and symbols.
- Never share passwords with others.
- Change passwords immediately if compromise is suspected.
- Use Multi-Factor Authentication (MFA) wherever available.
- Lock devices when unattended.

Passwords must not:

- Be written down where others can access them.
- Be shared via email or messaging systems.
- Be reused across multiple critical systems.

Device Security

The school will:

- Ensure all devices have up-to-date operating systems.
- Install security updates promptly.
- Maintain antivirus and malware protection.
- Use filtering and monitoring systems provided through Hwb and Local Authority services where applicable.
- Encrypt portable devices containing personal information.

Staff must:

- Not install unauthorised software.
- Use school-approved applications only.
- Report lost or stolen devices immediately.

Email Security

Staff should:

- Be alert to phishing emails.
- Verify unusual requests for information or payments.
- Avoid opening attachments or clicking links from unknown sources.
- Report suspicious emails immediately.

The school will provide guidance and training on identifying cyber threats.

Data Protection

The school will:

- Process personal data in accordance with UK GDPR and Data Protection legislation.
- Limit access to personal information on a need-to-know basis.
- Store information securely.
- Use approved systems for sharing sensitive information.

Staff must:

- Only access data required for their role.
- Avoid storing sensitive data unnecessarily.
- Follow data retention and disposal requirements.

Backup and Recovery

The school will:

- Ensure critical data is backed up regularly through Local Authority and approved cloud services.
- Test recovery procedures periodically.
- Maintain business continuity arrangements to minimise disruption following a cyber incident.

Remote Working

When working remotely, staff must:

- Use secure internet connections.
- Access systems through approved services such as Hwb and Local Authority platforms.
- Avoid using shared devices where possible.
- Ensure confidential information cannot be viewed by unauthorised individuals.

Cyber Security Education

The school will:

- Provide regular cyber security awareness training for staff.
- Promote online safety education for learners.

- Use Hwb resources and Welsh Government materials to develop digital resilience.
- Include cyber security awareness within the curriculum where appropriate.

Incident Reporting

A cyber security incident may include:

- Phishing attacks
- Malware infections
- Unauthorised access
- Data breaches
- Lost or stolen devices
- Suspicious system activity

All incidents must be reported immediately to:

1. The Headteacher
2. The school's IT support provider
3. The Data Protection Officer where personal data may be affected

The school will record and investigate all incidents and take appropriate remedial action.

Monitoring and Review

The school reserves the right to monitor the use of its ICT systems to:

- Maintain security
- Detect misuse
- Protect users and data
- Meet legal responsibilities

Monitoring will be conducted in accordance with data protection legislation.

Policy Review

This policy will be reviewed annually or sooner if:

- New cyber security threats emerge.
- Welsh Government guidance changes.
- Significant incidents occur.
- Legislative requirements change.

Policy Approved By: Governing Body – November 26 taking to GB meeting

Headteacher: 

Chair of Governors: _____

Date Approved:

29th September 2026