Archdiocese of Seattle

Incident Reporting from Parishes and Schools

This document outlines a reporting protocol to ensure timely, consistent, and effective response to cybersecurity incidents affecting archdiocesan parishes and schools. This is requested to protect sensitive data, minimize disruption and comply with regulatory, insurance and diocesan requirements. All staff, volunteers, and contractors at parishes and schools who use Archdiocesan IT systems, email, or data services are requested to follow these incident reporting procedures.

Definition of a Cybersecurity Incident
Any event that may compromise the confidentiality, integrity, or availability of information systems or data, including but not limited to:

- Phishing emails
- Ransomware or malware infections
- Unauthorized access or data breaches
- Lost or stolen devices
- Suspicious login attempts
- Website defacement or outages
- Request

All cybersecurity incidents should be reported immediately to the archdiocese's cybersecurity team via incident@seattlearch.org. The archdiocese will investigate, coordinate response efforts and provide guidance to affected entities.

Instructions for Reporting Cybersecurity Incidents
Please follow the simple steps to quickly report any cybersecurity incidents:

Step 1: Identify the incident - If you suspect or observe any of the following, it may be a cybersecurity incident:

- You received a suspicious email asking for credentials or payment.
- Your device is behaving abnormally (e.g., pop-ups, slow performance).
- You cannot access your email or systems.
- You notice unauthorized changes to files or accounts.
- You lost a device containing sensitive data.

Step 2: Report the incident- Send an email to incident@seattlearch.org with the following information:

- Subject Line: Cybersecurity Incident Report – [Parish/School Name]
- Email body:

    - Name of reporter
    - Parish/School name
    - Contact information (Phone & Email)
    - Date and time of incident
    - Type of incident (e.g., phishing, malware, unauthorized access)
    - Systems or data affected
    - How the incident was detected
    - Any immediate action taken
    - Screenshots or attachments (if applicable)
    - Additional notes or concerns

Step 3: Preserve evidence
Do not delete suspicious emails or files. Please take screenshots if possible and disconnect affected devices from the network if instructed.

Step 4: Await potential guidance
Based on the criticality of the incident, the archdiocese cybersecurity team may respond with next steps, which may include:

- Containment and recovery instructions
- Forensic investigation
- Communication templates for affected parties
- Recommendations for future prevention
- Teachable moment sharing request

When parish staff correctly identify a phishing email or suspicious link before interacting with it, they should report the incident through the standard reporting process (e.g., forward to the cybersecurity team or use the designated reporting tool). After reporting, they can share their experience as an example to create a learning opportunity with their team. This strengthens awareness and builds a culture of proactive cybersecurity. When sharing:

- Remove or disable the malicious link before distribution.
- Highlight key indicators of phishing (e.g., unusual sender, misspelled domain, urgent tone).
- Use approved communication channels (e.g., internal email, bulletin board, or collaboration platform).
- Frame the message as educational, not punitive.