All Saints Church School
A Bath and Wells Academy

Appendix 2 - Security Incident Management (SIM): Record of work

This document provides the documented evidence and audit trail of a reported information security incident. It is designed to operate alongside the organisation's Data Protection Policy, and Data Breach Policy.

This form is to be completed by the Incident Handler(s) in the organisation.

The incident may require additional input and support from the organisation's Data Protection Officer, ICT, and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s):	
Date reported to organisation:	
By whom:	
Date reported to Incident handler:	
By whom:	
Date incident occurred:	
Senior Management notified (date):	

Summary of breach:	

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	• Necessary staff trained on incident handling and incident response • Policy, Procedures & Guidance https://allsaintsprimary.j2bloggy.com/ • Network Diagrams are held by ICT • The Record of Processing Activities (RoPA) will provide details of data, owners, custodians, and third parties – link to the RoPA • ICT also record event logs and hold logs on other systems (e.g. emails, firewalls etc) • Key contacts: office@allsaints.bwmat.org
2. Identification Detect the incident – Is it an incident (breach of policy), a near miss, or a data breach? Determine its scope, and involve the appropriate parties	
3. Containment Contain the incident to minimize its	

effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for anything remaining	
5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	
6. Wrap Up Document the lessons learned and actions to reduce the risk of the incident/breach/near miss re-occurring Document the decision to report to both the affected data subjects and the ICO.	
	If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay **Decision to report to Data subjects** - Yes / No Based on: Officer: Signed: Date:
	Establish the likelihood and severity of the resulting risk to people's rights and freedoms - A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned **Decision to report to ICO** - Yes / No Based on: Officer: Signed: Date: