**Cyber Security Risk Assessment
Author: Dan Hilton, Head of IT**

**Date: 28th June 2024**

**Review Due: 28th June 2025**

As per the **DSAT Network / Data Incident Response Plan**, all suspected cyber incidents are to be reported to Nevine Towers and Dan Hilton with as much detail as possible. The steps outlined in the plan will then be followed.

This document aims to identify the specific cyber security risks faced by both schools within our Trust and the DSAT central team.

# Malicious Software

**Who might be harmed and how?**
All school electronic devices including the server could be infected. All staff could be impacted, the malware could be used to secretly gather data and send information to a third party.

**What are we doing?**
Windows machines are protected with Sophos Intercept X Advanced. Only supported version of Windows are in use. iPads and Chromebooks are managed centrally through MDM platforms and software has to be pushed out by the IT team. Staff receive cyber security training.

**Risk level**
**MEDIUM**

# Ransomware

**Who might be harmed and how?**Everyone on site could be affected. Staff could be denied access to files on their computers.

**What are we doing?**On site documents stored on the server are backed up to the cloud using Redstor Online Backup Service. These backups are air-gapped to give additional protection. Staff are encouraged keep personal files in Office 365 OneDrive and shared files in Office 365 SharePoint. This gives an additional level of protection as files can be restored to any point in the previous 30 days. Staff are trained not to open unknown, suspicious files as part of cyber security training.

**Risk level
HIGH**

# Loss Of Systems

**Who might be harmed and how?**Everyone on site could be affected. Staff could be denied access to files on their computers.

**What are we doing?**Servers are backed up both locally and to the cloud using Redstor. DSAT have an emergency server that can be moved to any site to restore services in the event of a server based network outage. In the event that schools Smoothwall firewall fails, we have a spare Smoothwall which can be put in place to restore internet connectivity.

**Risk Level
MEDIUM**

# Denial Of Service Attack (Dos / DDoS)

**Who might be harmed and how?**Everyone on site could be affected as the internet connection could be compromised to the extent that web site and cloud based services can’t be contacted.

**What are we doing?**Schools have a Smoothwall firewall which sits between the outside world and their internal network. The OS of the Smoothwall is kept up to date with latest patches. While we can’t stop DoS and DDoS attacks from happening – we can liaise with our partners Smoothwall and Virgin Media if one compromised our internet connectivity.

**What do we need to do?**Travis St. Lawrence & Swallownest don’t currently have a Smoothwall. They use an equivalent product that was installed by their previous IT support provider. They will be moving to a Smoothwall solution within the next year.

**Risk Level**
**LOW**

# Date Theft / Breach

**Who might be harmed and how?**Everyone could be affected. Breaches tend to occur due to either weaknesses in technology or user behaviour (or a combination of both).

**What are we doing?**

Staff receive training regarding phishing attacks as part of their cyber security training. User have unique logins and passwords and know not to write these passwords down or share them. Most users Office 365 accounts are protected with MFA (multifactor authentication)

**What do we need to do?**

Force MFA for all Office 365 users who don’t currently have it switched on.

**Risk Level**
**HIGH**

# Fraud / Financial Losses

**Who might be harmed and how?**While any member of staff could be targeted, school business managers are particularly vulnerable to this kind of attack. Phishing scams attempt to obtain financial information and may try and trick schools into making payments online.

**What are we doing?**

Staff are trained not to share login details and to be aware of phishing scams as part of their cyber security training.

**Risk Level
HIGH**

# Insider Threats

**Who might be harmed and how?**Everyone could be affected. Data could be stolen and passwords could be shared outside of DSAT.

**What are we doing?**

Staff receive GDPR training. When staff members leave, IT are informed and their email and network accounts are deleted or disabled promptly. Cloud based accounts must also be closed promptly when staff members leave.

**Risk Level**

**LOW**