THE DIOCESE OF SHEFFIELD ACADEMIES TRUST

NETWORK/DATA INCIDENT RESPONSE PLAN 2022-23

THE DIOCESE OF SHEFFIELD ACADEMIES TRUST

Approved by:	DSAT Trust Board
Last reviewed on:	
Next review due by:	

Network / Data Incident Response Plan

Author: Dan Hilton
Date: 22/09/2022
Version: 1.3

- IT Support Lead / Headteacher / Business Manager reports incident to Nevine Towers (NT) & Dan Hilton (DH) with as much detail as possible. Incident is declared.
- DH to establish the nature of the incident – this will generally be either a hardware / software failure or cyber security incident (the latter considered the most likely scenario).

Hardware / Software Failure

- DH to attend site to assess situation. Quick fix applied if possible (an example of this could be a faulty network switch or faulty UPS).
- If parts need to be ordered then network reconfigured to function in the absence of the main server until repair can be made.
- If parts cannot be obtained in a 48hr time period the DSAT emergency server VM can be deployed as a temporary measure. Server data can be restored to SharePoint and made available to staff via their Office 365 account.
- Headteacher to confirm to NT once the incident has been resolved.

Cyber Security Incident

- DH to establish the nature of the incident. Initially this may involve bringing the network down and removing people's access to network & cloud-based resources while the source of infection is identified and remedied.
- NT to report cyber security incident to National Cyber Security Centre: https://report.ncsc.gov.uk
- Clare Sturman to establish whether incident represents a GDPR breach and report to ICO if required: https://ico.org.uk/for-organisations/report-a-breach/
- NT to inform IT leads at other schools so they can check their systems are clean and rule out wider infection throughout the Trust.
- Affected data to be recovered from local backup is possible.
- Failing this, local data to be recovered from Redstor cloud-based backup to SharePoint and made available to staff via their Office 365 account (this may not be a complete restore as storage constraints mean historical data considered non-critical is routinely excluded).
- If server isn't operational the DSAT emergency server VM will be deployed as a temporary measure to restore vital services.
- If SharePoint data is affected by the incident then clean data is recovered by rolling back to a prior date.
- If SharePoint recovery fails via the admin panel options then a ticket is opened with Microsoft. They have the ability to roll back SharePoint data up to 12 days in the past.
- Once school's server is operational the emergency VM can either be migrated to the on-premises server or the school will revert to their previous setup.
- Headteacher to confirm to NT once the incident has been resolved.