CYBER RESPONSE PLAN

April 2023

Responsibility	Head Teacher
Date of next review by	31/03/2024

Signed:

Head Teacher

Date: 17/04/23

Signed:

Director of Lifelong Learning

Date: 17/04/23

Contents

1. INTRODUCTION

This Cyber Response Plan forms part of the overall continuity plan of the Academy and needs to ensure a minimum level of functionality to safeguard pupils and staff, and to restore the school back to an operational standard. In this regard this Cyber Response Plan should be considered as part of the Academy's **Critical Incident Management Policy for Disaster Recovery** and will be reviewed annually. Reference should also be made to the Academy's **Strategic Risk Register**.

The Academy is a member of the DfE's RPA (Risk Protection Arrangement) as such has implemented the following:

1.1. Offline IT backups through Redstor. When back-ups are taken, previous backups are not affected, allowing data to be recovered prior to any point,
1.2. Staff and Governors with access to the Academy's Management Information System(s) are required to complete the National Cyber Security Centre's training.
1.3. The Academy is registered with Police Cyber Alarm
1.4. IT users are required to sign the ICT acceptable use policy and Academy Code of Conduct, which includes loan devices.

This plan is to ensure that in the event of malicious cyber-attack, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

2. ACTIONS IN THE EVENT OF AN INCIDENT

In the event of a suspected incident of ransomware or another cyber incident, the following steps should be followed:

- Contact CSE (IT Support Provider) by telephone 01993 886688
- Contact the 24/7/365 RPA Cyber Emergency Assistance by telephone 0800 368 6378 or by e-mail: RPAresponse@CyberClan.com
- Inform the National Cyber Security Centre (NCSC): https://report.ncsc.gov.uk
- Contact local police via Action Fraud website https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime or telephone 0300 123 2040
- Contact the schools Data Protection Officer by telephone on 01629 532888 or e-mail to gdprforschools@derbyshire.gov.uk.
- DPO will advise whether ICO should be contacted (0303 123 1112)
- Contact Sector Security Enquires Team at the DfE: sector.securityenquiries@education.gov.uk

3. RECOVERY PLAN

In the event of a suspected cyber incident the Academy's IT Support provider (CSE) must be contacted immediately. If IT support is not on site they must be contacted on 01993 886688.

3.1. Verify initial incident and record on the **Incident Recovery Event Recording Form** (Appendix A).
3.2. Assess and document the scope of the incident using the **Incident Impact Assessment** (Appendix B) to identify which key functions are operational/which are affected.
3.3. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
3.4. In order to assist data recovery, if damage to a computer or backup material is suspected, staff **should not**:

- Turn off electrical power to any computer.
- Try to run any hard drive, backup disc to try and retrieve data.
- Tamper with or move damaged computers or discs.

3.5. Contact RPA Emergency Assistance Helpline (see Section 2 above for contact details).

3.6. Start the 'Actions Log' (Incident Recovery Event Recording Form) to record recovery steps and monitor progress.

3.7. Convene the Cyber Recovery Team (CRT), this will consist of:

- Head Teacher
- Deputy Head Teacher
- Director of Operations
- Director of Lifelong Learning
- Designated Safeguarding Lead
- CSE IT Support, on site engineer

3.8. Liaise with IT support to estimate recovery time and likely impact.

3.9. Make a decision as to the safety of the school remaining open: refer to **Critical Incident Management Policy for Disaster Recovery.**

3.10. Identify legal obligations and any required statutory reporting e.g. criminal acts, report to the Data Protection Officer in the event of a data breach.

3.11. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.

3.12. Upon completion of process, complete **Post Incident Evaluation** form to evaluate the effectiveness of the response (see Appendix C).

3.13. Educate employees (and pupils) on avoiding similar incidents/implements lessons learned.

4. CURRENT MITIGATIONS AGAINST CYBER ATTACK

The Academy currently employs the following mitigations against cyber security attack

- Microsoft Licences: All servers and PCs licencing kept fully up to date, enabling patch management (security updates) to be applied as/when required.
- CSE Magellan: Provides encryption when accessing files remotely.
- Redstor: Offline backups, protecting data in a location separate from the network. All data is backed up onto Redstor cloud platform, keeping entire network restorable should anything impact on the onsite server.
- Ransomware Scanning: Scans each backup within Redstor Data Centre each night checking for any dormant files.
- Smoothwall (Filter and Firewall): Firewall solution provides a hardware physical barrier between Academy and outside world. Filter solution provides a safe environment for internet searches and aids in blocking external software attacks.
- Sophos Intercept X: Protects each server and each client, scanning local devices for unwanted files and placing them into quarantine if deemed necessary and flagged to ICT Support for further investigation. Also provides a *'Paper Trail'* for identification of any source of threat.
- DarkWeb Analysis: Flags potential security concerns regarding available usernames and passwords of staff that become available on the 'Dark Web'.
- Phishing e-mail testing: DarkWeb analysis utilised to perform an agreed schedule of phishing email testing for staff users identifying any staff member that may require further training.
- Finance and Management Information System cloud based and remotely accessible.

- Protocols ensure website passwords are not automatically saved.
- Password protocol required passwords to be changed every 42 days with a mix of letters/numbers and characters.
- ICT Acceptable Use and ICT and E-Safety policies in place.
- Lockout Policy – 10 failed password attempts will result in the computer locking for 30 minutes.
- The names of all leavers are passed on to ICT support where their access to the school network is disabled.
- Cloud based access to the school MIS is disabled on the day the staff member leaves the school/their contract end date.
- All staff must only use their own admin account.
- E-mail alerts have been set up for all accounts using outside/external networks.

Appendix A: Incident Recovery Event Recording Form

Description or reference of disaster:	
Date of the incident:	
Date of the incident report:	
Date/time disaster recovery commenced:	
Date recovery work was completed:	
Was full recovery achieved?	

Relevant Referrals

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

Actions Log

Recovery Tasks (*In order of completion)*	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

Appendix B: Incident Impact Assessment

Operational	No Impact	There is no noticeable impact on the school's ability to function.
	Minor Impact	There is some loss in the ability to function which is minor. Functions can be carried out but may take longer and there is a loss of efficiency.
	Medium Impact	The school has lost the ability to provide some critical services (administration **or** teaching and learning) to **some** users. The loss of functionality is noticeable, but work arounds are possible with planning and additional resource.
	High Impact	The school can no longer provide any critical services to users. It is likely the school will close, or disruption will be considerable.

Informational	No Breach	No information has been accessed / compromised or lost.
	Data Breach	Access or loss of data which is **not** linked to individuals and classed as personal. This may include school action plans, lesson planning, policies and meeting notes.
	Personal Data Breach	Sensitive personally identifiable data has been accessed or extracted. Data which may cause 'significant impact' to the person / people concerned requires a report to the ICO within 72 hours.
	Integrity Loss	Data, which may include sensitive personal data, has been changed or deleted. (This also includes corruption of data)

Restoration	Existing Resources	Recovery can be promptly facilitated with the resources which are readily available to the school.
	Facilitated by Additional Resources	Recovery can be facilitated within an identified timescale with additional resources which can be easily accessed.
	Third Party Services	Recovery is not guaranteed, and outside services are required to facilitate full or partial restoration.
	Not Recoverable	Recovery from the incident is not possible. Data may have been extracted, encrypted or backups may have failed.

Appendix C: Post Incident Evaluation

Response Grades 1-5 1 = Poor, ineffective and slow 5 = Efficient, well communicated and effective.

Action	Response Grading	Comments for Improvements / Amendments
Initial Incident Notification		
Enactment of the Action plan		
Coordination of the Disaster Recovery Team		
Communications Strategy		
Impact minimisation		
Backup and restore processes		
Were contingency plans sufficient?		
Staff roles assigned and carried out correctly?		
Timescale for resolution / restore		
Was full recovery achieved?		
Log any requirements for additional training and suggested changes to policy / procedure:		