Risk Protection Arrangement Cyber response Plan

Edleston Primary School

November 2023

A Cyber Response Plan will be considered as part of an overall continuity plan that schools need to ensure they maintain a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

- If a school fails to plan effectively then recovery can be severely impacted, causing additional loss of data, time, and ultimately, reputation.
- Incidents may occur during the school day or out of hours. The Cyber Response Plan should be tested, with input from key stakeholders, to ensure that in an emergency there is a clear strategy, which has fail-safes when key personnel are unavailable.
- The plan should cover all essential and critical IT infrastructure, systems, and networks. The plan will ensure that communications can be quickly established whilst activating cyber recovery. It is also important that the plan is well communicated and readily available.
- The document is to ensure that in the event of a cyber-attack, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

Aims of a Cyber Response Plan

When developing a Cyber Response Plan, you will need to consider who will be involved in the Cyber Recovery Team, the key roles and responsibilities of staff, what data assets are critical and how long you would be able to function without each one, establish plans for internal and external communications and have thought about how you would access registers and staff and pupil contact details. This will allow the school:

- To ensure immediate and appropriate action is taken in the event of an IT incident.
- To enable prompt internal reporting and recording of incidents.
- To have immediate access to all relevant contact details (including backup services and IT technical support staff).
- To maintain the welfare of pupils and staff.
- To minimise disruption to the functioning of the school.
- To ensure that the school responds in a consistent and effective manner in order to reduce confusion and reactivity.
- To restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the school which are unaffected.

Risk Protection Arrangement Cover

From April 2022, the Risk Protection Arrangement (RPA) will include cover for Cyber Incidents, which is defined in the RPA Membership Rules as:

“Any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data.”

Your RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident, you must contact the RPA Emergency Assistance.

To be eligible for RPA Cyber cover, there are 4 conditions that members must meet:

Have offline backups. Help and guidance on backing up is available from the National Cyber Security Centre (NCSC) and should ideally follow the 3-2-1 rule explained in the NCSC blog Offline backups in an online world - NCSC.GOV.UK

It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups. Education providers should ask their IT teams or external IT providers to ensure the following:

a)Backing up the right data. Ensuring the right data is backed up paramount. See Critical Activities for a suggested list of data to include.

b) Backups are held fully offline and not connected to systems or in cold storage, ideally following the 3-2-1 rule explained in the NCSC blog Offline backups in an online world: https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

c) Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored, and data recovered from backups.

Further Help and guidance on backing up can be found at: Step 1 - Backing up your data - NCSC.GOV.UK. https://www.ncsc.gov.uk/collection/small-business- guide/backing-your-data

2. All Employees or Governors who have access to the Member's information technology system must undertake NCSC Cyber Security Training by the 31 May 2022 or the start of the Membership Year, whichever is later. Upon completion, a certificate can be downloaded by each person. In the event of a claim the Member will be required to provide this evidence.

3. Register with Police CyberAlarm. Registering will connect Members with their local police cyber protect team and in the majority of cases, a cyber-alarm software tool can be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data. When registering, use the code "RPA Member" in the Signup code box.

4. Have a Cyber Response Plan in place. This template is for you to use to draft a school- specific plan if you do not already have one. It can be downloaded from the RPA members portal.

For full terms and conditions of Cyber cover, please refer to the relevant Membership Rules on gov.uk.

Preparation and Additional Resources

Preventative Strategies

It is vital education providers regularly review their existing defenses and take the necessary steps to protect their networks. In addition to the 4 conditions of cover detailed above, there are several suggested measures that schools can implement to help themselves to improve their IT security and mitigate the risk of a cyber-attack:

- Regularly review IT Security Policy and Data Protection Policy.
- Assess the school's current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role based user access. Cyber Essentials is a government-backed baseline standard, which we would encourage all RPA members to strive towards achieving wherever possible.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.
- Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis. Vulnerabilities within Microsoft Exchange Servers have been the root cause of many cyber-attacks in the last six months. It is highly recommended that on-premises exchange servers are reviewed and patched/updated as a high priority and moving to an Office 365 environment with MFA if possible.
- Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are:
- If external RDP connections are used, MFA should be used
- Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
- Enable an account lockout policy for failed attempts
- The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended
- Review NCSC advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks - NCSC.GOV.UK
- Provide awareness training for staff to recognise, report, appropriately respond to security messages and/or suspicious activities.

Advice and Guidance

The NCSC website has an extensive range of practical resources to help improve Cyber Security for Schools - NCSC.GOV.UK

Acceptable use

Ensure all users have read the relevant policies and signed IT acceptable use and loan agreements for school devices. Please be aware if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the police.

Communicating the Plan

Communicate the Cyber Recovery Plan to all those who are likely to be affected and be sure to inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.

Testing and Review

During an incident there can be many actions to complete, and each step should be well thought out, cohesive, and ordered logically.

Train key staff members to feel confident following and implementing the plan. Review the plan regularly to ensure contact details are up-to-date and new systems have been included. NCSC have resources to test your incident response with an Exercise in a Box - NCSC.GOV.UK

Making Templates readily available

It is recommended that templates are available to cover reporting, recording, logging incidents and actions, and communicating to stakeholders.

Actions in the event if an Incident.

If you suspect you have been the victim of a ransomware or other cyber incident, you should take the following steps immediately:

- Enact your Cyber Recovery Plan
- Contact the 24/7/365 RPA Cyber Emergency Assistance:
- By telephone: **0800 368 6378** or by email: **RPAresponse@CyberClan.com**
- You will receive a guaranteed response within 15 minutes
- Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible
- Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including: forensic investigation services and support in bringing IT operations securely back up and running.
- Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk
- Contact your local police via Action Fraud Action Fraud website or call **0300 123 2040**
- If you are a part of a Local Authority (LA), they should be contacted
- Contact your Data Protection Officer
- Consider whether reporting to the ICO is necessary report at www.ico.org.uk **0303 123 1112**
- Contact the Sector Security Enquiries Team at the Department for Education by emailing:sector.securityenquiries@education.gov.uk

Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.

Cyber Recovery Plan

1. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
2. Assess and document the scope of the incident using the Incident Impact Assessment at Appendix A to identify which key functions are operational / which are affected.
3. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
4. In order to assist data recovery, if damage to a computer or back up material is suspected,

staff **should not:**

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

5. Contact RPA Emergency Assistance Helpline.
6. Start the Actions Log to record recovery steps and monitor progress.
7. Convene the Cyber Recovery Team (CRT).
8. Liaise with IT staff to estimate the recovery time and likely impact.
9. Make a decision as to the safety of the school remaining open.

This will be in liaison with relevant Local Authority Support Services / Trust

10. Identify legal obligations and any required statutory reporting e.g., criminal acts / reports to the Information Commissioner's Office in the event of a data breach.

• *This may involve the school's Data Protection Officer and the police*

11. Execute the communication strategy which should include a media / press release if applicable.

• *Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.*

12. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
13. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix D and review the Cyber Recovery Plan accordingly.
14. Educate employees on avoiding similar incidents / implement lessons learned.

Key Roles and Responsibilities

Every school is unique and the structure and staffing levels will determine who will be assigned which task. This example will help you assign roles and responsibilities, but this is not an exhaustive or a definitive list.

Headteacher (with support from Deputy Head)

- Seeks clarification from person notifying incident.
- Sets up and maintains an incident log, including dates / times and actions.
- Convenes the Cyber Recovery Team (CRT) to inform of incident and enact the plan.
- Liaises with the Chair of Governors.
- Liaises with the school Data Protection Officer.
- Convenes and informs staff, advising them to follow the 'script' when discussing the incident.
- Prepares relevant statements / letters for the media, parents / pupils.
- Liaises with School Business Officer / Manager to contact parents, if required, as necessary

Designated Safeguarding Lead (DSL)

- Seeks clarification as to whether there is a safeguarding aspect to the incident.
- Considers whether a referral to Cyber Protect Officers / Early Help / Social Services is required.

Site Manager / Caretaker

- Ensures site access for external IT staff.
- Liaises with the Headteacher to ensure access is limited to essential personnel.

School Business Officer / Manager

- Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
- Ensures office staff understand the standard response and knows who the media contact within school is.
- Contacts relevant external agencies – RPA Emergency Assistance / IT services / technical support staff
- Manages the communications, website / texts to parents / school emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

Data Protection Officer (DPO)

- Supports the school, using the school data map and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- Liaises with the Headteacher / Chair of Governors and determines if a report to the ICO is necessary.
- Advises on the appropriateness of any plans for temporary access / systems.

Chair of Governors

- Supports the Headteacher throughout the process and ensure decisions are based on sound judgement and relevant advice.
- Understands there may be a need to make additional funds available and have a process to approve this.
- Ensures all governors are aware of the situation and are advised not to comment to third parties / the media.
- Reviews the response after the incident to consider changes to working practices or school policy.

IT Lead / IT Staff

Depending upon whether the school has internal or outsourced IT provision, the roles for IT Co- ordinators and technical support staff will differ.

- Verifies the most recent and successful backup.
- Liaises with the RPA Incident Response Service to assess whether the backup can be restored or if server(s) themselves are damaged, restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss.
- Liaises with the Headteacher as to the likely cost of repair / restore / required hardware purchase. Provides an estimate of any downtime and advises which systems are affected / unaffected.
- If necessary, arranges for access to the off-site backup.
- Protects any records which have not been affected.

  Ensures on-going access to unaffected records.

Teaching Staff and Teaching Assistants

- Reassures pupils, staying within agreed pupil standard response
- Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed

Critical Activities – Data Assets

All of the following data can either backed up remotely or on site and can be returned either from stored or remote/back up or from the cloud. Any back-ups that are not logged into ie Teachers to Parents for text messaging etc will need to be retrieved by ICT Services at County ICT service desk. 0300 13 5121

Activities

- Exam entries and controlled assessments
- Assessment and Exams
- Targets, assessment and tracking data
- Baseline and prior attainment records
- Exam timetables and cover provision

Exam results

- School development plans
- Policies and procedures

Governance

- Governors meeting dates / calendar
- Governor attendance and training records
- Governors minutes and agendas

Admissions information

- School to school transfers
- Transition information
- Contact details of pupils and parents

Administration

- Access to absence reporting systems
- School diary of appointments / meetings
- Pupil timetables
- Letters to parents / newsletters
- Extra-curricular activity timetable and contacts for providers
- Census records and statutory return data
- Payroll systems
- Human Resources
- Staff attendance, absences, and reporting facilities
- Disciplinary / grievance records
- Staff timetables and any cover arrangements
- Contact details of staff
- Photocopying / printing provision
- Telecoms - school phones and access to answerphone messages
- Email - access to school email systems

Office Management

- School website and any website chat functions / contact forms
- Social media accounts (Facebook / Twitter)
- Management Information System (MIS)
- School text messaging system
- School payments system (for parents)
- Financial Management System - access for orders / purchases
- Visitor sign in / sign out
- CCTV access

Site Management

- Site maps

- Maintenance logs, including legionella and fire records
- Risk assessments and risk management systems
- COSHH register and asbestos register

Catering Records

- Contact information for catering staff
- Supplier contact details
- Payment records for food & drink
- Special dietary requirements / allergies
- Stock taking and orders

The full details of contact names, addresses, telephone numbers/email and account numbers are held in the full policy no published in accordance with the Data Protection Act 2018 and adhering to the schools Data Sharing policy. http://www.edleston.cheshire.sch.uk/serve_file/3169263