CYBER RESPONSE PLAN

for adoption by all CDAT schools

This policy is informed by the Christian values which are the basis for all of CDAT's work and any actions taken under this policy will reflect this.

'Blessed are those who act justly, who always do what is right'

Psalm 106:3

Approved by	Date	Review Schedule	Date of next review
Trust Board	1 March 2024	Annually	March 2025

What is the purpose of our Cyber Response Plan?

1.1. This Cyber Response Plan is part of our overall continuity plans to ensure that CDAT schools maintain a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard following a relevant Cyber Incident. Our continuity plans enable our schools to plan effectively for recovery to minimise the impacts on loss of data, time, and ultimately, reputation.

1.2. This Cyber Response Plan covers all essential and critical IT infrastructure, systems, and networks for any incidents that may occur during the school day or out of hours. It seeks to ensure that communications can be quickly established whilst activating cyber recovery.

1.3. Ultimately this document is to ensure that in the event of a Cyber Incident attack, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

1.4. It is imperative that this plan should be communicated and readily available to all those who are likely to be affected, and to inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.

1.5. More specifically, this Cyber Response Plan seeks to allow our schools:

1.5.1. To ensure immediate and appropriate action is taken in the event of a Cyber Incident.
1.5.2. To enable prompt internal reporting and recording of incidents.
1.5.3. To have immediate access to all relevant contact details (including backup services and IT technical support staff).
1.5.4. To maintain the welfare of pupils and staff.
1.5.5. To minimise disruption to the functioning of our schools.
1.5.6. To ensure that our staff respond in a consistent and effective manner in order to reduce confusion and reactivity.
1.5.7. To restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the school which are unaffected.

2. What is a Cyber Incident?

2.1. From April 2022, our Risk Protection Arrangement (RPA) includes a 24/7 dedicated helpline and dedicated email address to cover Cyber Incidents, which are 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.*"

2.2. Essentially this means that a Cyber Incident occurs if there is any unauthorised access to any school device and/or any school data.

2.3. 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.

2.4. If you know of, or suspect that, such an incident has occurred you must act immediately and follow the steps contained in this plan.

3. What steps are we taking to prevent a Cyber Incident?

3.1. We regularly review our Information Security Policy, Acceptable Use Policy, and Data Protection Policy.

3.2. We assess security measures against the Cyber Essentials requirements, such as firewall rules, malware protection, and role-based user access.

3.3. We are working to ensure that Multi-Factor Authentication (MFA) is in place to confirm a user's identity by using a combination of two or more different factors.

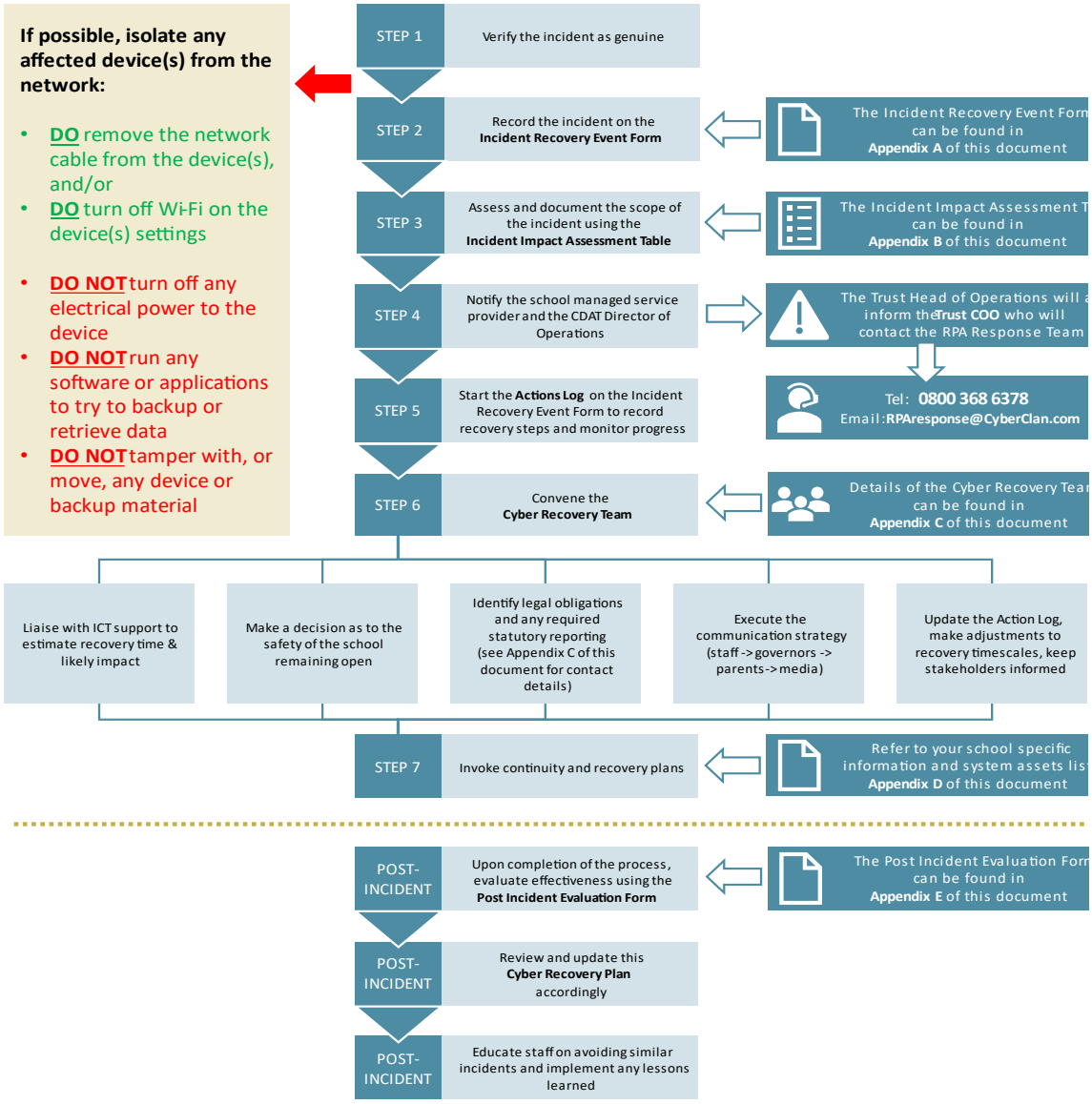
3.4. School ICT Managed Service providers should implement a regular patching regime to routinely install security and system updates and ensure any internet-facing device is not susceptible to an exploit.

3.5. We are considering, through the development of our CDAT ICT strategy, approaches to minimising the risks presented by on-premise servers.

3.6. We no longer allow the use of external RDP access to devices within the central team.

4. What steps need to be taken in the event of a Cyber Incident?

The following steps must be taken by the Headteacher (or nominated Deputy) upon receiving notification or referral of an actual or suspected Cyber Incident:



What are the roles and responsibilities in relation to this Cyber Response Plan?

4.1. **Headteacher / Head of School** (with support from delegated support)

- 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.
- Provides a summary of the incident to the Director of Operations, by phone, if systems are compromised.
- 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 administration staff to contact parents, if required, as necessary.

4.2. **Director of Operations**

- Seeks clarification from Headteacher on all incident log items.
- Supports the Headteacher in completing the paperwork and enact the plan.
- Organises the CRT and designs the next steps.
- Liaises with the DPO as required.
- Liaises with the CEO where escalation is required.
- Owns the relationship, communications, and liaison with RPA.
- Oversees the reporting and response to a Cyber Incident.
- Is a senior stakeholder within the Cyber Recovery Team (CRT).

4.3. **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 / Local Authority Social Care Services is required.

4.4. **Site Manager / Caretaker** (where applicable)

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

4.5. **School Bursar / Business Manager / Administration Officer** (where applicable)

- Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
- Ensures office staff understand the standard response for media enquiries.
- Assesses whether payroll or HR functions are affected and considers if additional support is required, liaising with the Director of Finance where required.

4.6. **Data Protection Officer (DPO)**

- Supports the Director of Operations, 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 Director of Operations to determine if a report to the ICO is necessary.
- Advises on the appropriateness of any plans for temporary access / systems.

4.7. **ICT Managed Service Representative**

- 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 Director of Finance 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.

4.8. **Teaching Staff and Teaching Assistants**

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

Appendix A: Incident Recovery Event Recording Form

CDAT Cyber Response Plan: Cyber Incident Recovery Event Recording Form	
Incident Overview	
Description or reference of incident:	
Date/time the incident occurred:	
Date/time the incident was reported:	
Date/time incident recovery commenced:	
Date/time recovery work was completed:	
Was full recovery achieved?	

Relevant Referrals

Referred to	Contact details	Contacted on (date/time)	Contacted by	Response

Actions Log

Recovery Task	Owner	Completion Date		Comments	Outcome
		Estimated	Actual		

Appendix B: Incident Impact Assessment Table

Use this table to assess and document the scope of the incident in order to identify which key functions remain operational and which are affected:

CDAT Cyber Response Plan: Incident Impact Assessment	
OPERATIONS	
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.
DATA & INFORMATION	
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 & RECOVERY	
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: Cyber Recovery Team & Other Relevant Contacts

In the event of this plan having to be initiated, the personnel named below will form the Cyber Recovery Team and take control of the aspects identified. Where there is school-specific information (e.g. managed service provider) please add local information as appropriate:

CDAT Cyber Response Plan: CYBER RECOVERY TEAM			
Reference	**Name**	**Role in Trust/School**	**Contact Details**
DOO	Chris Williams	Director of Operations	chris.williams@cdat.co.uk 07488811916
CEO	Neil Dixon	Chief Executive Officer	neil.dixon@cdat.co.uk
ICT Managed Service	[school to insert details]	[school to insert details]	[school to insert details]

Key suppliers who may need to be involved in Recovery planning are as follows:

CDAT Cyber Response Plan: KEY CONTACTS		
Supplier	**Contact Name / Tel Number**	**Account / Reference Number**
ICT Managed Service Provider	[school to insert details]	[school to insert details]
Website Host	[school to insert details]	[school to insert details]
Electricity Supplier	[school to insert details]	[school to insert details]
Burglar Alarm	[school to insert details]	[school to insert details]
Action Fraud	0300 123 2040	https://www.actionfraud.police.uk/reporting-fraud-
Local Constabulary	0300 123 2040	https://www.actionfraud.police.uk/reporting-fraud-
Legal Representative	Stone King	LauraBerman@stoneking.co.uk
DPO	Veritau	schoolsDPO@veritau.co.uk

The following agencies may require notification of a Cyber Incident. Communications should be handled in accordance with the relevant steps in this plan and also via the Cyber Response Team once it has been convened:

CDAT Cyber Response Plan: LEGAL AND STATUTORY CONTACTS	
Organisation	**Contact Details**
RPA Cyber Emergency Assistance	Telephone: 0800 368 6378 Email: RPAresponse@CyberClan.com
National Cyber Security Centre (NCSC)	Report at: https://report.ncsc.gov.uk
Local police via Action Fraud	Telephone: 0300 123 2040 Website: https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime
Information Commissioners Office (ICO)	Telephone: 0300 123 1112 Website: https://www.ico.org.uk
DfE Sector Securities Enquiry Team	Email: sector.securityenquiries@education.gov.uk

Appendix D: School specific Information and System Assets Lists

[Schools are required to complete the tables within this Appendix]

Critical Activities - Data Assets

List all the data assets your school has access to and decide which are critical and how long you would be able to function without each one. This could be a matter of a few hours or a matter of a day, a week or even a month. Complete the required column with the timescale you believe is necessary for recovery (e.g. 4hrs / 12hrs / 24hrs / 48hrs / 72 hrs / 1 week / 2 weeks / 3 weeks / 1 month). Also decide if there are any temporary workarounds and consider the cost of any additional resources which may be required in an emergency situation.

Critical Activities	**Item required for service continuity** ***(add/delete as required)***	**When Required**	**Workaround? (Yes / No)**
Leadership and Management	Access to Headteacher's email address		
	Minutes of SLT meetings and agendas		
	Head's reports to governors (past and present)		
	Key stage, departmental and class information		
Safeguarding / Welfare	Access to reporting & recording of safeguarding concerns		
	Attendance registers		
	Class groups / teaching groups, and staff timetables		
	Referral information / outside agency / TAFs		
	Child protection records		
	Looked After Children (LAC) records / PEPs		
	Pupil Premium pupils and funding allocations		
	Pastoral records and welfare information		
Medical	Access to medical conditions information		
	Administration of Medicines Record		
	First Aid / Accident Logs		
Teaching	Schemes of work, lesson plans and objectives		
	Seating plans		
	Teaching resources, such as worksheets		
	Learning platform / online homework platform		
	Curriculum learning apps and online resources		
	CPD / staff training records		
	Pupil reports and parental communications		
SEND Data	SEND List and records of provision		
	Accessibility tools		
	Access arrangements and adjustments		
	IEPs / EHCPs / GRIPS		
Conduct and Behaviour	Reward system records (incl. house or conduct points)		
	Behaviour system records (incl. negative behaviour points)		
	Sanctions		
	Exclusion records, past and current		
	Behavioural observations / staff notes and incident records		

Critical Activities	Data item required for service continuity *(add/delete as required)*	When Required	Workaround? (Yes / No)
Assessment and SATs	SATs entries and controlled assessments		
	Targets, assessment, and tracking data		
	Baseline and prior attainment records		
	SATs results		
Governance	School development plans		
	Policies and procedures		
	Governor's meeting dates / calendar		
	Governor attendance and training records		
	Governors' minutes and agendas		
Administration	Admissions information		
	School to school transfers		
	Transition information		
	Contact details of pupils and parents		
	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		
Human Resources	Payroll systems		
	Staff attendance, absences, and reporting facilities		
	Disciplinary / grievance records		
	Staff timetables and any cover arrangements		
	Contact details of staff		
Office Management	Photocopying / printing provision		
	Telecoms - school phones & access to answerphone		
	Email - access to school email systems		
	School website and any chat functions / contact forms		
	Social media accounts (Facebook / Twitter)		
	Management Information System (MIS)		
	School text messaging system		
	School payments system (for parents)		
	Finance system - access for orders / purchases		
Site Management	Visitors sign in / sign out		
	CCTV access		
	Site maps		
	Maintenance logs, including legionella and fire records		
	Risk assessments and risk management systems		
	COSHH register and asbestos register		
Catering	Contact information for catering staff		
	Supplier contact details		
	Payment records for food & drink		
	Special dietary requirements / allergies		
	Stock taking and orders		

Server Access

Please detail all the people with administrative access to the server(s):

Role	Name	Contact Details
[school to insert details]	[school to insert details]	[school to insert details]

Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS (add rows as required) [school to insert details]:

MIS Admin Access	Name	Contact Details
Headteacher		
Other School Staff		
MIS Provider		
CDAT		

Backup Strategy

Please detail all the current arrangements for backup of information, data, and systems [school to insert details]:

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server		
School MIS		
Cloud Services		
Third Party Applications / Software		
Email Server		
Curriculum Files		
Administration Files		
Finance / Purchasing	Access	
HR / Personnel Records		
Safeguarding		
Budgeting	Access	
H&S System	Smartlog	

Appendix E: Post Incident Evaluation Form

(Response Grading 1-5, from 1=”Poor, ineffective and slow” through to 5=”Efficient, well communicated and effective”)

CDAT Cyber Response Plan: Post Incident Evaluation		
Action	**Response Grading**	**Comments for Improvements / Amendments**
Initial Incident Notification		
Enactment of the Action plan		
Co-ordination of the Cyber 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:		