DDAT

Derby Diocesan Academy Trust

Cyber Response and Recovery Plan

Approved by the Trust Board on: 18th July 2023

Introduction

This DDAT cyber response and recovery plan has been designed to be a supplement to your school's existing Cyber-security Policy. The aim of a cyber response and recovery plan is to assess which data assets are critical, the length of time the school would be able to function without access to certain data, determine how communication will be managed, and establish a back-up strategy.

This plan should be read in conjunction with the DDAT Social Media Policy and includes:

- Plan details
- Plan testing details
- Contact information
- Cyber recovery team information
- Critical data assets
- Back-up strategy
- Media contact strategy
- Stakeholder contact strategy
- Communication action plan
- Recovery action plan
- Incident reporting form
- Post incident evaluation report

Cyber response and recovery plan

Important: Do not share this plan with members of the public or leave it unattended, as it contains confidential information. You must also remain vigilant about who can access this plan, as the plan has the potential to be used with malicious intent, e.g. cyber attacks.

Document information	
Name of school	
Name of trust	Derby Diocesan Academy Trust

Testing details	
Cyber response and recovery plan	
Date plan was last tested	
Test approved by	
Date of next test	
Person responsible for next testing	
Back-up strategy	
Date back-up strategy was last tested	
Test approved by	
Date of next test	
Person responsible for next testing	

1. Contact information

School contact information	
Name of school	
School address	
School contact number	
School contact email address	
Name of Headteacher / Executive Headteacher	
Headteacher / Executive Headteacher contact number	
Headteacher / Executive Headteacher email address	

Insurance contact information	
Name of insurance provider	RPA
Contact number of insurance provider	0800 368 6378
Email address of insurance provider	RPAresponse@Cyberclan.com
Operating hours	24 hours per day 365 days per year

2. Response team contact and access information

The tables below outline the roles and contact numbers of those involved in the cyber recovery team. Other roles and responsibilities surrounding cyber security and recovery can be found in the school's Cyber Security Policy which can be accessed via Trust website.

Cyber recovery team

Role	Name	Contact number/email address
In the event of a breach, the personnel named below will form the cyber recovery team and enact the roles listed.		
Incident Response Leader	Dr Sarah Clark (CEO)	07568 109789 Sarah.Clark@ddat.org.uk
Deputy Response Leader	Hayley Wharton (COO)	07710 122995 Hayley.Wharton@ddat.org.uk
Technical Lead	Mark Fryers Link ICT	
Data Protection Officer	Jason Hampton	DDATAdmin@ddat.org.uk
Headteacher/Executive Headteacher	As per websites	
Public relations manager	Contact COO	
IT Technicians		
DfE incident support helpline		0800 046 8687 Monday to Friday, 8:00am-4:00pm

3. Critical data assets

Below are the Trust / school's critical data assets. The table shows the level of risk the Trust / school faces in losing access to each type of information, whether it is considered critical information, the estimated time the Trust / school could function without access, and whether there is a work-around solution in place should access be lost.

The risk of disruption to the access of each type of information has been indicated using the following risk matrix:

Risk rating		Likelihood of occurrence		
		Probable	**Possible**	**Remote**
Likely impact	**Major**	High	High	Medium
	Severe	High	Medium	Low
	Minor	Medium	Low	Low

This information is updated annually and approved by the Headteacher / Executive Headteacher / CEO and ICT Manager.

Data asset	Risk of disruption to usual route to this information	Critical information? Y/N	Estimated time back-up access could be lost without disruption	Workaround in place? Y/N
Leadership and management				
Access to Headteacher / Executive Headteacher / CEO / DCEO / CFO / COO email address				

Minutes of Executive / SLT meetings and agendas				
Trustee / Governor reports				
Key stage, department and class information				
Class groups				
Staff timetables				
Safeguarding and welfare				
Access to safeguarding reporting systems				
Access to safeguarding concerns already registered				
Attendance registers				
Safeguarding referral information				
Child protection records				

LAC and previously LAC records				
Records of pupils eligible for pupil premium and their funding allocations				
Pastoral records and welfare information				
Medical and first aid				
Pupil medical information				
Pupil allergen information				
IHPs				
Staff medical information				
Staff allergen information				
Administration of medicines records				
First aid administration logs				
Accident logs				

Teaching and learning				
Lesson plans and objectives				
Classroom seating plans				
Curriculum maps and planning				
Teaching and learning apps and online resources				
School learning platforms				
Homework platforms				
CPD and staff training records				
Pupil reports				
SEND and accessibility				
Records of pupils with SEND				
Records of individual pupil needs				

Accessibility tools				
Access arrangements and adjustments				
EHC plans				
Behaviour and exclusions				
Reward system records, e.g. house points				
Behaviour records and records of sanctions implemented				
Exclusion records, past and current				
Individual pupil behaviour notes and staff observations				
Behaviour incident records				
Exams and assessments				

Data on exam entries and controlled assessments				
Targets, assessment and tracking data				
Baseline and prior attainment records				
Exam and assessment timetables				
Exam and assessment results				
Governance				
SDP data				
Policies and procedures				
Trustee / Governing board meeting dates and calendar				
Trustee / Governor attendance records				

Trustee / Governor training records				
Trustee / Governing board minutes				
Trustee / Governing board agendas				
Administration				
Admissions information				
School-to-school transfer information				
Transition information				
Parent and pupil contact information				
Absence reporting systems				
School diary and calendar				
Pupil timetables				

Parent communications, e.g. letters and newsletters				
School prospectus				
Extra-curricular timetables				
Extra-curricular provider contact details				
Census data and records				
Other statutory return data				
HR				
Payroll systems				
Staff attendance and absence data				
Disciplinary and grievance records				
Staff timetables				
Cover arrangements				

Staff contact details				
Office administration and social media				
Photocopying and printing provision				
Trust / School email systems				
Trust / School website				
Social media accounts				
MIS				
School text messaging system				
Payment systems, e.g. for parents				
Financial systems, e.g. purchasing				
Online banking				
Site management				
Visitor logs				

CCTV access				
Maintenance logs				
Fire safety records				
Legionella records				
Risk assessments				
Asbestos register				
COSHH register				
Site maps				
Suppliers and contractors				
Order and work records				
Supplier and contractor contact details				
Supplier and contractor payment records				

4. Back-up strategy

Below is the Trust's / school's back-up strategy. It shows where certain back-up information is held, who it is held by (including third party holders), the frequency that it is backed up, whether it is considered critical information, and an estimate for how long the Trust / school could manage without access to this information before the loss of access would cause disruption.

The risk of disruption to the usual route of access to this information and the risk of disruption to the back-up location of this information has been indicated using the following risk matrix:

Risk rating		Likelihood of occurrence		
		Probable	**Possible**	**Remote**
Likely impact	**Major**	High	High	Medium
	Severe	High	Medium	Low
	Minor	Medium	Low	Low

This information is updated annually and approved by the Headteacher / Executive Headteacher / CEO and ICT manager.

Pupil information

Information type	Risk of disruption to usual route to this information	Back-up type	Back-up provider	Back-up location	Frequency of back-up	Critical information? Y/N	Estimated time back-up access could be lost without disruption	Risk of disruption to back-up route to this information
Pupil attendance registers	Medium	Online cloud storage	Provider name	Off-site	Monthly	Y	24 hours	Low
Admissions register								
Pupils' contact details								
Pupils' emergency contact details								
Current child protection concerns								
Child protection concerns records								

Staff information

Information type	Risk of disruption to usual route to this information	Back-up type	Back-up provider	Back-up location	Frequency of back-up	Critical information? Y/N	Estimated time back-up access could be lost without disruption	Risk of disruption to back-up route to this information
Personnel records								
SCR								
Staff contact details								
Staff emergency contact details								
Information held on staff work devices								

Trust / School information

Information type	Risk of disruption to usual route to this information	Back-up type	Back-up provider	Back-up location	Frequency of back-up	Critical information? Y/N	Estimated time back-up access could be lost without disruption	Risk of disruption to back-up route to this information
Main filer server								
School MIS								
Cloud services								
Third-party software								
Email server								
Curriculum information								
Administration files								
Financial information								

Purchasing information								
Asset information								
Inventory								
Facilities management information								
Bookings and lettings information								
Trust / School website								
USBs and other portable storage devices								

5. Media contact

Important: If you have **not** been assigned media liaison responsibilities, you **should not** respond to requests from the media for information about the breach, or the Trust's / school's response to the breach. Instead, you should refer any enquiries to media representative to the members of staff included in the table below.

Name	Role	Contact number
Only the personnel named below will have assigned media liaison responsibilities		
Sarah Clark	CEO	07568 109789
Hayley Wharton	COO	07710 122995
	Headteacher / Executive Headteacher after liaising with CEO or COO	

The assigned members of staff will liaise with the media, working to the Trust's / school's agreed procedures. Assigned staff will provide verified facts only and are encouraged to state that they do not know an answer to an enquiry instead of offering speculation.

Be aware that media enquiries can come in many forms and will ask various versions of key questions. Key questions can be broken down into:

- What has happened?
- What was compromised?
- How did the incident happen?
- What will the Trust / school do to address the incident?

Only assigned staff will liaise with the media and offer answers to such questions at an agreed point in time.

Important: The Headteacher / Executive Headteacher / CEO must be notified as soon as possible in the event that an unauthorised staff member has spoken with the press against the agreed Trust / school procedures.

6. Internal and parent communications

Method and timeframes

The table below shows who is responsible for communicating with key stakeholders about the cyber incident and the timeframe by which the Trust / school has agreed this should be enacted.

Group	Who will notify them	Method of notification	Timeframe
Pupils	Headteacher / Executive Headteacher	Assembly	Within 24 hours
Staff	Headteacher / Executive Headteacher / CEO / COO	Staff meeting	ASAP
Trustees / Governors	Headteacher / Executive Headteacher / CEO	Board / LGB meeting	ASAP
Parents	Headteacher / Executive Headteacher	Message / letter to parents if required	Within 24 hours

Back-up contact information

The table below shows the direct location of where back-up contact information for each stakeholder group is stored and who has access to this information, in the event that usual access routes to this contact information has been disrupted.

Group	Location of back-up communications information	Access rights
Pupils	Cloud storage	Headteacher / Executive Headteacher
Staff	Cloud storage	Headteacher / Executive Headteacher / CEO / Executive Team
Trustees / Governors	Cloud storage	Headteacher / Executive Headteacher / CEO / Executive Team
Parents	Paper contact cards	Headteacher / Executive Headteacher / School Office

7. Actions in the event of an incident – communication

In the event that the school suspects it has been a victim of ransomware or another cyber incident, e.g. data breach, follow the steps below immediately.

Please be aware that enacting these actions as soon as possible is of critical importance.

These steps will be undertaken by the Headteacher / Executive Headteacher / CEO / COO in the event of an incident.

Initial actions

1. • Ensure you have all the incident information you are likely to need as quickly as possible – this helps to confirm the validity of the claim and ensure the next steps can be enacted without delay.
2. • Contact the risk protection arrangement (RPA) emergency assistance helpline on **0800 368 6378** or via RPAresponse@CyberClan.com as soon as possible.
3. • Follow any instructions given to you by the helpline, as required.

Reporting

1. Inform the National Cyber Security Centre (NCSC) as soon as possible via the online form: https://report.ncsc.gov.uk
2. Contact the local police via the action fraud telephone line on **0300 123 2040**.
3. Contact the ICO, where necessary, e.g. if there has been a data breach, via the online form (https://ico.org.uk/for-organisations/report-a-breach) or **0303 123 1112**.

Further contact

1. Inform any relevant Trust / school insurance providers and follow their instructions.
2. Inform DDAT.
3. Contact the Secter Securities Enquiries Team and the DfE via sector.securityenquiries@education.gov.uk.

8. Actions in response to an incident – recovery

These actions will be undertaken by the Headteacher / Executive Headteacher / CEO / COO / ICT Manager in the event of an incident.

Follow the processes listed below once you have verified the incident as genuine and identified what areas of cybersecurity have been affected.

Reference number	Description of action	Tick when complete
1	Where required, e.g. during a cyber attack, isolate all devices from the affected network.	
2	Assess whether electrical power to devices should remain on; however, **do not** turn off the power to a device if damage to the device or back-up material is suspected.	
3	Communicate to staff **not** to run any hard-drives, back-up discs, or try to retrieve data until instructed that it is safe to do so.	
4	Communicate to staff **not** to move or tamper with any devices or device components until instructed that it is safe to do so.	
5	Ensure the communication steps outlined in section 8 of this plan have been followed before continuing.	
6	Begin recording your recovery steps and monitor recovery progress.	
7	Convene the cyber response team.	
8	Liaise with ICT staff to estimate the recovery time and likely impact.	
9	Assess the safety of the Trust / school and decide, with the advice of the trust whether the school can remain open.	
10	Where there has been a crime committed, ensure this has been reported the police.	
11	Where a data breach has occurred, ensure this has been reported to the ICO.	
12	Identify whether any other statutory reporting requirements are required and have been carried out.	

14	Ensure the following groups of stakeholders have been made aware of the incident, in the following order: 1. Staff 2. Governors 3. Parents and pupils	
15	Execute the media communication strategy, where required. Do not inform the media prior to informing your school's stakeholders.	
16	Assess the timescales needed for recovery and ensure stakeholders have been informed.	
17	Evaluate the effectiveness of the cyber response and recovery plan and ensure processes are put in place for it to be reviewed.	
18	Implement a 'lessons learnt' strategy to minimise the risk of the incident reoccurring.	

9. Cyber incident recording form

Use the tables below to ensure the necessary information about the incident has been recorded.

Incident details

Reference number	Description of action
Description or reference of incident	
Date of incident	
Date incident reported	
Date recovery commenced	
Date recovery completed	
Was full recovery achieved?	
If not, what was not recovered and why?	

Referrals

Referral to	Contacted on	Contacted by	Referrer response

Actions log

Fill out the table below in the order of tasks completed during the incident.

Action	Person responsible	Completion date	Outcome

10. Post incident evaluation report

Complete the table below using the following grading system. Ensure you add any comments about how to amend or improve the action for future use if you did not grade it a 5.

Grading

Grade	Meaning	Example scenario
1	Failed	The response was completely ineffective, not followed through, not communicated, or was the incorrect response to this type of incident.
2	Poor	The response was largely ineffective, slow, poorly communicated, or was mostly an incorrect response to this type of incident.
3	Satisfactory	The response was somewhat effective, but timing or communication could be improved upon. It may not have been the most appropriate response, but some positive results were observed.
4	Good	The response was mostly effective, timing and communication were efficient but could be improved upon. It was the correct response to this type of incident and positive results were mostly observed.
5	Excellent	The response was highly effective, and timing and communication were very efficient. This was the best possible response to this type of incident and positive results were observed.

Action or strategy	Response grading	Comments for improvements and/or amendments
Initial incident notification		
Enactment of the cyber response action plan		
Coordination of the cyber recovery team		

Communication with stakeholders		
Communication with external agencies		
Impact minimisation strategies		
Back-up strategies		
Contingency planning		
Roles within the cyber response team		
Timescales for recovery		
Additional questions		
Was full recovery achieved?		
Why do you think full recovery was/was not achieved?		
Are there any training requirements needed as a result of this incident?		
Why do you think additional training is/is not required?		
Are any changes to school policy and procedures needed as a result of this incident?		
Why do you think changes to school policy are/are not needed?		
What are the lessons learnt upon reflection of this incident?		
Post incident report completed by		
Date		

An Equality Impact Assessment has been completed for this policy.