Built on botheredness . . .

the enquire learning trust

Cyber Response Plan

Contents

Version History

Approved by:	Trustees
Last reviewed:	June 2025
Next review due by:	Sept 2026

Date	Author	Version	Comment
September 2024	BW		New policy
June 2025	BW		Reviewed – no changes

1. Introduction

This Cyber Response Plan supplements the overall continuity plan of the Trust and it's Academies and needs to ensure a minimum level of functionality to safeguard pupils and staff, and to restore the school back to an operational standard should a cyber threat materialise.

In this regard this Cyber Response Plan should be considered as part of the Trust's Disaster Recovery Policy and will be reviewed annually. Reference has also been made to the Trust's Risk Register.

All ELT Academies are members of the DfE's RPA (Risk Protection Arrangement) and as such have implemented the following:

- Offline IT back-ups through Redstor. When back-ups are taken, previous back-ups are not affected, allowing data to be recovered prior to any point with unlimited retention available.
- All Staff and AIC members are required to complete the National Cyber Security Centre's training which is set within Flick, our training platform, and forms part of the Trust's induction checklist for all staff and governance members.
- All ELT Academies are registered with the Police Cyber Alarm
- Staff and student users of ICT are required to sign the ICT acceptable use policy as well as completing the Information Governance Policy training element in Flick which outlines what devices are allowed to be used, how, when, and by who.

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 other cyber incident, the following steps should be immediately followed:

- Contact Brett Webster (Director of Information Technology) by telephone on 07545134955
- Report the breach/potential breach using the Data Breach form on our GDPR site - https://enquirelearningtrust.sharepoint.com/sites/UKGDPR/SitePages/Forms.aspx - which upon completion will also inform Liz Thompson (Trust DPO)
- After the Director of IT has reviewed the incident, dependant on severity, he may:
    - Inform the schools local IT Support provider for further support and assistance onsite where needed
    - 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 Sector Security Enquires Team at the DfE: sector.securityenquiries@education.gov.uk

3. Recovery plan

In the event of a suspected cyber incident the Trust's Director of IT (Brett Webster) must be contacted immediately by phone on 07545134955. If for any reason there is no response, please report this to your local IT Support provider.

- Verify and review initial incident and record reported by the school logged on the Data Breach form here - https://enquirelearningtrust.sharepoint.com/sites/UKGDPR/SitePages/Forms.aspx
- Assess and document the scope of the incident using the Incident Impact Assessment (Appendix A) to identify which key functions are operational/which are affected.
- In the event of a suspected cyber-attack, IT Support staff will isolate devices from the network under the instruction from the Trust Director of IT.
- Now that all Trust data, email included, is stored within our Office 365 tenancy online, recovery of any data isn't reliant on onsite equipment, servers or backup media. Recovery of any data required can be done instantly without the need for additional replacement hardware.
- Dependent upon severity, contact the RPA Emergency Assistance Helpline (see Section 2 above for contact details).
- Convene a Cyber Recovery Team, this will consist of the personnel below to outline the steps and timescales to restore access to systems impacted;
  • Principal
  • Business Manager
  • Director of Information Technology
  • Director of Governance
  • School IT Support provider
- Start recovery of data, email or other online services impacted
- Liaise with IT support for any onsite actions required dependant on system and service breached
- Make a decision as to the safety of the school remaining open: refer to the Trust Disaster Recovery Policy and liaise with Trust Director of Operations and CEO.
- 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.
- Make adjustments if necessary to recovery timescales as time progresses and keep all stakeholders informed.
- Upon completion of process, complete Post Incident Evaluation form to evaluate the effectiveness of the response (see Appendix B).
- Educate employees (and pupils) on avoiding similar incidents/implements lessons learned either in person or by reassigning Flick training relevant to Cyber Security.

4. Current mitigations against Cyber Attack

The Trust currently employs the following mitigations against cyber security attack:

- Microsoft Licences: All servers, laptops and computer licences allow us to keep fully up to date, enabling patch management (security updates) to be applied upon release. Windows 11 is installed Trust wide with no alternate versions of OS allowed on the network.
- Office 365 2FA: Provides multi-factor authentication when accessing files remotely and securely via our Office 365 tenancy. No data is stored locally or any device or copied out of the O365 environment.

- Redstor: Offline backups, protecting data in a location separate from the network. All data, emails, Teams and SharePoint is backed up onto Redstor cloud platform, keeping entire estate restorable should anything impact onsite. The local server has no reliance now on data.
- Ransomware Scanning: Scans each backup within Redstor Data Centre each night checking for any dormant files.
- Barracuda Total Protection: Integrates within our Office 365 tenancy to scan all inbound emails, checking for ransomware, phishing and malware related threats via email. Settings configured to quarantine and block harmful emails. This system also allows for remediation should any threats become active by searching for emails and user accounts infiltrated, deleting, clearing any further emails created (additional malware), and then informing users who may have been further exposed that these emails have been deleted automatically for their safety. Continued remediation for prolonged periods of time can be setup too dependent on severity, continually looking for similar/same threats and stopping them at source.
- Meraki Firewall: Firewall solution provides a hardware physical barrier between Academy and outside world and is configured to block all inbound as well as only allowing specific outbound requests pertinent to the services and systems we use as a Trust. An underpinning 'Deny All' rule is set for anything outbound other than the the systems we authorise the use of.
- Securly (Filter and Aware): Filter solution provides a safe environment for internet searches and aids in blocking external software attacks.
- BitDefender Endpoint: Anti-virus protection for each server and each Windows and Apple client, scanning local devices for unwanted files and placing them into quarantine if deemed necessary and flagged to the Director of IT for further investigation. Also provides a 'Audit Trail' for identification of any source of threat to support investigation if required.
- Phishing e-mail testing: Barracuda Phishline utilised to perform an agreed schedule of phishing email testing for staff users identifying any staff member that may require further training – undertaken at least annually.
- Finance, Payroll and Management Information Systems all cloud based and remotely accessible with backups provided against SLA from vendor.
- Password protocol require passwords to be changed regular – dependant on system - but all with a mix of letters/numbers and characters.
- Information Governance, including Information Security and Acceptable Use as well as Online Safety policies all in place.
- The names of all leavers are passed on to IT support where their access to the school network is disabled upon leaving. From September 2025 this will be automated where when staff contracts end or students become off-roll on Bromcom, this will then disable their computer and Office 365 accounts.
- Cloud based access to the school MIS is disabled on the day the staff member leaves the school/their contract end date by the system administrators at school level – Business Manager and Principal.
- All staff must only use their own account and sharing credentials is in breach of the Information Governance Policy.

Appendix A: 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 B: 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 and detail provided		
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:		