# Crofty Education Trust

## CYBER RESPONSE PLAN

Date of Drafting: March 2025

Adopted Date: September 2025

Review Date: September 2026

# Contents

## Introduction

A Cyber Response Plan should 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.

This document covers the high-level approach across the trust, and guidance as to how this should be applied to each school.

The document is to ensure that in the event of a cyberattack, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

**Academies should keep a paper copy of the plan, plus the related completed appendices, in a secure location, for use in the event of a loss of service incident.**

## Aims of a Cyber Response Plan

- 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:

1. 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 is 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

## Incident Classification

| Category | Definition | Examples |
|---|---|---|
| **C1** | Security incident resulting in Trust wide total loss of services, Trust wide data breach, or creating a trust wide safeguarding risk | Ransomware infection across central tenancy.<br>Loss of trust wide data store to unauthorised 3rd party.<br>Breach of trust wide access control, such that additional access can be granted.<br>Unauthorised user gains root/admin access to central tenancy |
| **C2** | Security incident resulting in a school wide total loss of services, School wide data breach, or creating a trust wide safeguarding risk | Ransomware infection across Isolated school tenancy.<br>Loss of School wide data store to unauthorised 3rd party.<br>Breach of school wide access control, such that additional access can be granted.<br>Unauthorised user gains root/admin access to School tenancy |
| | Security incident resulting in a partial loss of services within the trust, Individual data breaches of high-risk individuals within the trust | Ransomware infection within infrastructure preventing use of some services.<br>Breach of data or account security involving Executives, headteachers or department heads.<br>Partial breach of data such as Payroll |
| **C3** | Security incident resulting in a partial loss of services within a school | Ransomware infection within infrastructure preventing use of some services. |
| | Security incident confined to large numbers (20+) of low-risk staff endpoints | |
| **C4** | Security incident confined to medium numbers (5-20) of low-risk staff endpoints | |
| | Security incident confined to large numbers (20+) of low-risk Student endpoints | |
| **C5** | Security incident confined to small numbers (1-5) of low-risk staff endpoints | |
| | Security incident confined to medium numbers (5-20) of low-risk student endpoints | |
| **C6** | Security incident confined to small numbers (1-5) of low-risk student endpoints | |

# Identification of key personnel

## Incident Response Team

| Job Title | Responsibility | Categories | Scope |
|---|---|---|---|
| **IT Manager** | Lead incident response and ensures appropriate team is convened | C1 – C3 | Trust |
| **IT Network Manager** | Coordinate incident response resources | C1 – C6 | School/Trust |
| **CEO/Deputy CEO** | | C1 – C2 | Trust |
| **School leadership** | Implements contingency plans and supports resolution activities | C1 – C4 | School |
| **DPO** | Advise on data breaches | Where appropriate | School/Trust |
| **Education Directorate** | Support on mitigating educational impact of incident and recovery measures | As appropriate | School |
| **Finance Directorate** | Support school / trust with business decisions during recovery | As appropriate | School/Trust |
| **Estates team** | Building security and impact | As appropriate | School/Trust |
| **Safeguarding team** | Seeks clarification on safeguarding impact. Considers whether referral to cyber protect officers/Early Help/Social Services is required | As appropriate | School/Trust |

## Communication

Communications will be agreed by the response team and issued to office managers for distribution at school level, using the templates in appendix B.

Media communications will be managed by assigned staff, working to trust guidelines and using the approved templates.

Only verified facts should be included within communications to staff, parents or via the media.

## Legal and DPO

The trust DPO, School Pro TLC, should be contacted in the event of suspected or confirmed loss of data.

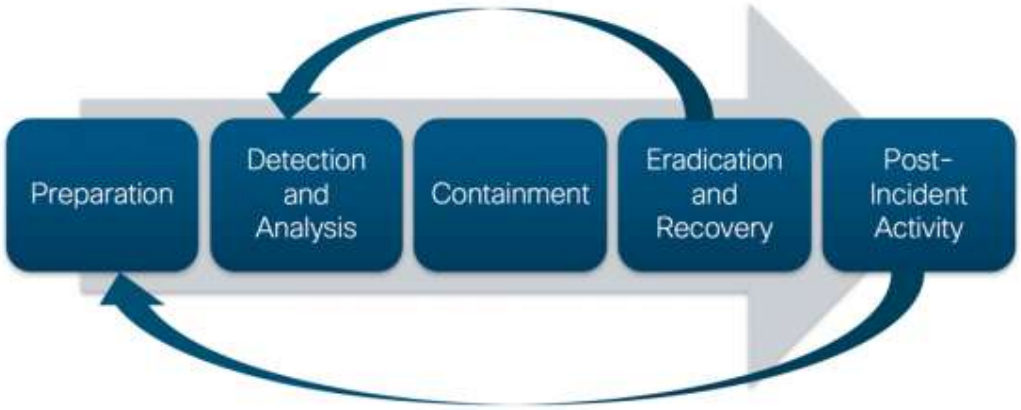
## IT

- 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 response team 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

# Incident Response Procedures




## Preparation

### Critical Activities

For each academy within the Trust, the Data Assets list (appendix E), backup matrix (appendix F), and Key contacts (appendix G) should be completed and maintained, detailing the criticality of each item, required recovery times and any workarounds.

Central IT will review the list, identify any further workarounds or gaps that could prevent recovery of that data asset during the required time, and propose resolutions/mitigations. If these are not accepted, the academy would be required to identify, document and implement alternative resolutions or amend the recovery times.

### Network Security

All academies will have a fully managed external firewall and filtering solution in place, with appropriate monitoring in place in line with the DfE connectivity guidelines, and appropriately budgeted for within the academy budget.

### Backups

All academies will have appropriate backups of critical infrastructure and data assets in place, in line with DfE and RPA guidelines. These backups should follow the 3-2-1 rule and include both offline and offsite copies of data, and backups should be automated, monitored and recovery tested.

This should be appropriately budgeted for within the academy budget.

### Antivirus/Anti Malware

Antivirus software must be installed and active on relevant endpoints and servers across the estate.

The trust is currently in Year 2 of a 3-year agreement for Kaspersky Endpoint Security maintained by Croft MSP (formerly NCI Technologies).

### Acceptable use

Academies will ensure all staff have read and signed IT acceptable use policies and ensure these are enforced appropriately.

Central IT will implement appropriate technical restrictions where possible to support this.

Users should use Multifactor authentication where this is available.

## Identifying and Reporting cyber incidents

1. Verify the initial incident report as genuine, and record on the incident recovery form (Appendix C).

2. Make an initial assessment of the scope of the incident using the Incident Impact Assessment (Appendix A) to determine priority, and then for:
   a. C1-C2 incidents, contact IT Manager
   b. C3-C6 incidents, contact IT Network Manager

3. IT will assess and convene response team as appropriate, and advise of initial rough order of magnitude recovery times

4. RPA emergency assistance helpline will be contacted as appropriate

5. Start action log

6. Implement responses and mitigations for impacts on education and learning.

## Isolating and containing cyber incident

In the event of suspected or confirmed compromise of systems or accounts, the following actions will be taken:

- Affected devices will be isolated from rest of network
- Affected user accounts will be blocked
- Affected network or cloud resources will be blocked.
- Checks undertaken for wider impact/infection

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, back up disc or tape to try and retrieve data
- Tamper with or move damaged computers, discs or tapes

## Analysing and assessing cyber incident

Once initial containment is complete, IT will coordinate the technical assessment of the cyber incident to determine next steps, removal of infection/risk and preventing reoccurrence.

The exact nature of this will vary based on the nature and requirements of the incident.

## Recovering from a cyber incident

### Immediate Mitigation

- Academy will implement contingency, mitigation and work around approaches as defined during preparation for impacted services and assets, while respecting any restrictions put in place as part of containment.
- Issue communications in line with policy using templates in Appendix B as appropriate.
- IT will support mitigation approaches while working on full resolution and ensure on-going access to unimpacted systems and data.

### Recovery

- Repair and disinfect impacted equipment if possible.
- Restore data from on site or offsite backups as possible.
- Focus on recovery of key systems in priority order.