Upload your school logo here.

Right-click and select change picture.

Cyber Response Plan
(Insert name of school or trust)

DFE URN Number		
Plan created	Date:	
Last reviewed	Date:	
Reviewed by		Date:
Signed and approved by head teacher		Date:
Signed and approved by Trust Board/ Governing Body		Date
Next review	Date:	

This document has contact information. It should only be shared with the people named in the school's Cyber Recovery Team.

Store this plan in a secure, accessible online location and keep an up-to-date hard copy as well.

Purpose

Your cyber response plan (CRP) is your guidance in the event of a cyber incident. It should be adapted to your school.

Cyber recovery team

These people are your school's cyber recovery team. They will manage a cyber incident, including deciding:

- what actions are needed to manage the incident
- timescales for actions
- third parties that need to be involved
- how often the team needs to meet
- how information will be communicated to the school and wider community.

Your school may have a third-party IT supplier or local authority (LA) service level agreement (SLA) or an incident response company who will support you if an incident happens. This may be your insurance provider, such as DfE Risk Protection Arrangement (RPA).

	Name	24-hour contact details (email/mobile)
Cyber recovery team leader/Meeting chair (SLT digital lead)		
Headteacher or designated member of SLT		
School's cyber lead		
SLT data protection officer		
Designated safeguarding lead (DSL)		
School business manager or support officer		

Administrator – to record minutes and actions		
Cyber incident response company		
IT provider / partner		
LA lead contact for safeguarding		
LA lead contact for legal and comms		
Insurance Provider		

If the cyber incident means you might need to close the school, take advice from the headteacher then discuss with the local authority and chair of trustees/governors.

Infrastructure, comms room, server, cloud storage and other IT access

These people may need to be contacted during a cyber incident. They can provide administrative access to the school's digital infrastructure, comms rooms, server or cloud storage solutions.

Role	Name	24-hour contact details (email/mobile)
Headteacher or designated member of SLT		
School business manager or school support officer		
IT provider		
Third-party IT provider		
Site manager or key holder		

Management information system (MIS) admin access

These people will provide administrative access to the school's MIS.

MIS admin access	Name	24-hour contact details (email/mobile)
Headteacher		
School business manager or school support		

officer		
MIS provider		
LA MIS link officer		
Third-party IT provider		
Data manager		

Other contacts

Depending on your circumstance, these individuals and organisations may be key business continuity contacts for the school. It is essential that all parties understand how to communicate with each other and the extent of their responsibilities.

Supplier	24-hour contact	Account / Reference number (if applicable)
Internet provider		
Backup internet provider		
Internal network provider		
Backup provider		
Telephony provider		
Website host		
CCTV supplier		
Electricity supplier		
Intruder alarm provider		
Text messaging system		
School catering provider		
Fire alarm provider		
Lift alarm provider		
Door entry access provider		
Fire Officer		

Useful reporting numbers

ICO	https://ico.org.uk/for-organisations/report-a-breach/
Action Fraud	**0300 123 2040**
NCSC	https://signpost-cyber-incident.service.gov.uk/
Local Police	Local police contact number
RPA	**0800 368 6378** rpa.dfe@education.gov.uk

Media contacts

These people will support with any media response.

Role	Name	Contact number/email
School media lead		
Local authority communications team		
Legal team (LA/Trust)		

Cyber communication plan

You need to have a cyber communication plan ready to be used in an incident. Sample communication templates are provided at the end of this document. These should be:

- edited to fit your school and circumstances
- approved by management and key leadership
- agreed with the relevant incident response stakeholders
- placed in a secure location, accessible even in the event of IT service failures

These templates can also be found at: https://cyber-security-hub.education.gov.uk/communication-templates

Critical information recovery - data assets

Identify the school's data assets and:

- which assets are critical
- how long the school can function without them
- temporary workarounds or if outsourcing is possible

Needed within

Decide how quickly you need access to each asset. Note if the asset is needed within:

- up to 4 hours
- 12 hours
- 24 hours
- 48 hours
- 72 hours
- 1 week
- 2 weeks
- 3 weeks
- 4 weeks

Criticality levels

Decide the criticality of each asset to your school. Use the following scale:

- low: school can operate with minimal disruption to daily functions
- moderate: school can operate but with more significant disruption to daily functions
- high: school cannot reasonably, safely operate without this function

Leadership and management

	Needed within	Criticality	Workaround (yes/no and add details)
Access to headteacher's email			
Minutes of SLT meetings and agendas			
Headteacher's reports to governors			

School self-evaluation data			
Key stage, departmental and class information			

Safeguarding and welfare

	Needed within	Criticality	Workaround (yes/no and add details)
Student records and contact information			
Systems to report and record safeguarding concerns			
Attendance registers			
Class/teaching groups and staff timetables			
Referral information/outside agency support and involvement			
Child protection records			
Looked after children records			
Eligibility for free school meals			
Pastoral records and welfare information			

Medical information

	Needed within	Criticality	Workaround (yes/no and details)
Medical conditions information			
Administration of medicines record			
First aid/accident logs			

Teaching

	Needed within	Criticality	Workaround (yes/no and details)
Schemes of work, lesson plans and objectives			
Seating plans			
Teaching resources (like worksheets)			
Learning/online homework platforms			
Curriculum learning apps and online resources			
CPD/staff training records			
Learner reports and parental communications			

Conduct and Behaviour

	Needed within	Criticality	Workaround (yes/no and details)
Reward system, including year/class/house points or conduct points			
Behaviour system, including negative behaviour points			
Sanctions			
Exclusion records (past and current)			
Records of racism and other incidents related to a protected characteristic			
Behavioural observations, staff notes and incident records			

Assessment and exams

	Needed within	Criticality	Workaround (yes/no and details)
Exam entries and controlled assessments			

Targets, assessment and tracking data			
Baseline and prior attainment records			
Exam timetables and cover provision			
Exam results			

Governance

	Needed within	Criticality	Workaround (yes/no and details)
School development plans			
Policies and procedures			
Governors' meetings dates/calendar			
Governors' attendance and training records			
Governors' minutes and agendas			

Formatted Table

Administration

	Needed within	Criticality	Workaround (yes/no and details)
Admissions information			
School to school transfers			
Transitions information			
Contact details of learners and parents			
Absence reporting systems			
School diary of appointments and meetings			
Learner timetables			
Letters/newsletters to parents			
Extra-curricular activity timetable and contacts for providers			

Census records and statutory return data			

Human resources

	Needed within	Criticality	Workaround (yes/no and details)
Payroll systems			
Staff attendance, absences, and reporting			
Arrangements for covering absent staff			
Disciplinary and grievance records			
Staff timetables			
Performance management records			
Staff contact details			

Office management

	Needed within	Criticality	Workaround (yes/no and details)
Photocopy and printing provision			
Telephony - school phones and access to answerphone messages			
School email systems			
School website, website chat functions, contact forms			
Social media accounts			
Management information system			
Text messaging system			
Payment system (for parents)			
Financial Management System - access for orders / purchases			

Site management

	Needed within	Criticality	Workaround (yes/no and details)
Visitor sign in and 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

	Needed within	Criticality	Workaround (yes/no and details)
Contact information for catering providers			
School meals payment records and systems			
Special dietary requirements and allergies			

Record keeping

Keep records during an incident to make sure the appropriate and correct steps are taken.

Guidance on record keeping: https://cyber-security-hub.education.gov.uk/record-keeping-in-an-incident

Decide which of these records you need to keep, bearing in mind your legal and regulatory requirements and your school setting.

Print out any templates or logs and add them to the hard copy of this document. Include links in case you are able to work online in an actual incident.

Template or log	Purpose	Link or hard Copy
Initial incident report	Description of incident, how it was discovered and the initial	

	assessment	
Incident log/timeline	Chronological list of actions, decisions and timestamps	
Communications log	Internal/external comms, such as emails, calls and in-person briefings	
Decision log	Rationale for decisions and who made them	
Technical forensic logs	System activity, logs from affected devices/networks	
Containment and recovery actions	Details of containment, mitigation and recovery efforts	
Data breach records	Personal data affected, DPO assessment and evidence of ICO notification	
Meeting notes	Summaries of strategy meetings or incident reviews	
Post-incident review report	Summary, lessons learnt and recommendations	
Follow-up actions tracker	Status of recommended improvements and action owners	

Incident response best practice

Adapt these actions to meet your school's requirements. Leave an action blank if it doesn't apply to your school. Make sure each process is agreed and approved by a member of your SLT.

Incident-specific guidance

DfE has playbooks for particular types of incidents. It is likely that they will be introduced at the triage stage of the process. Adapt the actions in the playbooks to fit your school and IT provider.

https://cyber-security-hub.education.gov.uk/processes-for-cyber-incidents

Detection and reporting procedure

Explain how you will detect and manage initial reports of cyber incidents.

Information on detection and reporting: https://cyber-security-hub.education.gov.uk/irp-detection-and-reporting-process

1. Detection

Decide what you will do when a report or alert is first received.

Your process:
Person responsible:

2. Logging

Start recording in your incident log. There is one included at the end of this plan.

Your process:
Person responsible:

3. Initial assessment

The person who identified the incident makes an initial assessment, with support from IT or other relevant people. Record this in an initial incident report.

Your process:I
Person responsible:

4. Decision to escalate response

Decide if the incident should be escalated immediately to a full incident response and involve SLT Digital Lead. This should be done if defined conditions (for example, harm to wellbeing, financial crime) are met.

Your process:
Person responsible:

5. SLT digital lead notification to escalate response

The SLT digital lead initiates the incident management processes and contacts the relevant people. Use the contact information tables to contact the correct people.

Your process:
Person responsible:

Triage and classification

Establish what sort of incident is occurring and its impact.

Information on triage and classification: https://cyber-security-hub.education.gov.uk/irp-triage-and-analysis

1. Preparation

Get the right people involved (SLT Digital Lead, IT Support, other stakeholders) and agree how you will communicate.

Your process:
Person responsible:

2. Investigation

Consider:

- what was observed or reported?
- when did it occur?
- who is affected?
- what systems or data are involved?
- could it be a known threat type?
- root cause analysis, if possible at this stage

Your process:
Person responsible:

3. Assign severity rating

Assign a priority level based on impact and urgency. You may update this later.

Your process:
Person responsible:

4. Action decision

Confirmation

Once the incident is identified, continue your cyber response process. Use the relevant playbook if applicable and agree actions to proceed with your response. If it is a high severity incident, you may need to bring in external support.

Unclear

If the cause of the incident is unclear, your SLT digital lead should escalate to SLT and initiate further investigation by the cyber recovery team. If it is a high severity incident, you may need to bring in external support.

Not a security incident

If it is not a security incident, record and either hand over any relevant records to another stakeholder or close the incident.

Your process:
Person responsible:

Containment

The purpose of containment is to:

- limit the spread of the incident
- preserve evidence
- minimise disruption
- protect sensitive data

Some of these suggested actions are very technical. If you have external technical support, they may perform these actions on your behalf. You will need to involve your technical experts (internal or external).

Make sure your SLT digital lead understands what activities and actions will be completed by your IT service provider or external technical support, and what actions should be completed internally. We have included suggested actions but there may be others you need to take.

Information on containment: https://cyber-security-hub.education.gov.uk/irp-containment

1. Identify the affected systems and scope

Use logs, alerts, user reports, or information from external parties.

Your process:
Person responsible:

2. Isolate affected systems or accounts

With IT support:

- remove affected or suspected devices from the network
- disable compromised user accounts and document sharing

Your process:
Person responsible:

3. Prevent further spread

With IT support:

- apply firewall rules
- disable infected services or applications

- temporarily suspend automatic syncs or backups

Your process:
Person responsible:

4. Preserve evidence

With IT support:

- capture volatile data such as logs
- save relevant emails, alerts, or error messages.
- label and store any devices removed from service, if applicable.

Your process:
Person responsible:

5. Communicate

SLT digital lead and cyber recovery team prepare updates to inform SLT, staff and external stakeholders.

Your process:
Person responsible:

Eradication

The eradication phase is about:

- removing the cause and any leftover components of a cyber security incident
- making sure it can't happen again through the same mechanism

Some of these suggested actions are very technical. If you have external technical support, they may perform these actions on your behalf. You will need to involve your technical experts, whether internal or external.

Make sure your SLT digital lead understands what activities and actions will be completed by your IT service provider or external technical support, and what actions should be completed internally. We have included suggested actions but there may be others you need to take.

Information on eradication: https://cyber-security-hub.education.gov.uk/irp-eradication

1. Re-confirm scope of affected systems

Check again which systems, users, and networks were affected.

Your process:

Person responsible:

2. Remove malware or malicious artefacts

Ask IT support to perform deep scans using up-to-date tools. If a full wipe is not possible, delete or quarantine. Scan for and remove:

- identified malware files
- malicious scripts
- PowerShell commands
- unauthorised binaries
- suspicious scheduled tasks, registry entries or run keys

Your process:
Person responsible:

3. Disable and replace compromised accounts

If you haven't already, you should:

- reset or disable any accounts you suspect have been compromised (follow your authorisation processes)
- reissue credentials, using strong password policies and multi-factor authentication (if possible)
- audit recent activity from any compromised accounts and check for any unauthorised movement or access

Your process:
Person responsible:

4. Patch and harden vulnerable systems

Check for and apply missing security patches or configuration changes to remove the attacker's access vector across the network and all devices. Harden system configurations, enforce principle of least privilege and close any unnecessary firewall ports or disable unused services.

Your process:
Person responsible:

5. Review and update security rules

Record and block known indicators of compromise and add newly discovered ones to security rules.

Your process:

Person responsible:

6. Clear temporary access or exceptions

Remove any short-term workarounds created during the containment phase, such as bypassed restrictions and emergency accounts. Document all changes and confirm their removal.

Your process:
Person responsible:

7. Re-test systems for clean status

Re-scan systems post-eradication. Use different tools or techniques than those during initial scans to increase detection coverage if possible.

Your process:
Person responsible:

Recovery

Recovery focuses on restoring affected systems, data, and services to business as usual in a secure and controlled way.

Information on recovery: https://cyber-security-hub.education.gov.uk/irp-recovery

1. System restoration

Rebuild affected systems from known good images or reinstall the operating system, where feasible. Restore essential data from secure, validated backups. Ensure restored systems are fully patched and up to date.

Your process:
Person responsible:

2. Integrity verification

Conduct full system scans using anti-virus and endpoint detection and response tools post-restoration. Validate key files, configurations, and applications are untampered using file integrity monitoring where available.

Your process:
Person responsible:

3. Credential reset and access control review

Require password changes for affected users. Enforce multi-factor authentication where supported, especially for admin or sensitive email accounts. Review and adjust user permissions if accounts were escalated or misused.

Your process:
Person responsible:

4. Controlled reintroduction of services

Bring systems back online in phases (not all at once), prioritising essential services. Continue containment restrictions during a phased return, if needed.

Your process:
Person responsible:

5. Testing and user validation

Perform basic system functionality checks. Ask key users to verify data accuracy and operational stability, running tests on critical systems if possible.

Your process:
Person responsible:

6. Monitor for reinfection or abnormalities

Discuss the possibility of increased monitoring with your IT support.

Your process:
Person responsible:

7. Communicate service status

Let staff and stakeholders know which systems have been restored. Provide guidance on safe system use and any new procedures. Flag systems that are still under restoration, or any additional steps being taken.

Your process:
Person responsible:

Notification

Notification is your communications during an incident response process.

Information on notification: https://cyber-security-hub.education.gov.uk/irp-notification

Actions to take

Decide:

- ❑ if a notification is needed, based on the data involved in the incident, the severity and scope
- ❑ who to notify (for example students, staff, parents and carers, governors, third parties, local authority)

If applicable, notify:

- ❑ internal stakeholders (for example safeguarding, pastoral, HR, finance)
- ❑ external bodies (for example ICO, DfE, police, insurers, IT providers)
- ❑ affected individuals (by letter, email, or phone call following GDPR guidance)
- ❑ the ICO if there is a personal data breach likely to result in risk to individuals – the ICO has guidance on when to report an incident
- ❑ your local authority, depending on contractual obligations or funding arrangements
- ❑ the police or action fraud, for cybercrime like ransomware, hacking, or financial fraud, or any direct threat to life or child wellbeing
- ❑ parents and guardians, when children's data is involved or there is safeguarding impact

You should also:

- ❑ log all notifications, including when they were sent, how, to who, and what the message was
- ❑ prepare press, website, or social media messaging if needed

Your process:
Person responsible:

Post-incident review

Evaluate the effectiveness of the incident response and any lessons learned, and make changes to reduce the likelihood and impact of future incidents.

Information on post-incident: https://cyber-security-hub.education.gov.uk/irp-post-incident

After an incident you should:

- evaluate how effective your incident response and management were
- identify lessons learned
- make improvements that reduce the likelihood and impact of future incidents

Actions to take

- ❑ hold a post-incident review within 5 to 10 working days of the incident closure
- ❑ collate all incident logs and evidence, including timelines, response steps and communication logs
- ❑ document the root cause and contributing factors, using available technical and procedural evidence
- ❑ assess the timeline of detection, escalation, containment, and recovery and identify any delays, inefficiencies or technical issues
- ❑ review internal and external communications and effectiveness
- ❑ identify any policy or procedure gaps - for staff, technical teams, or leadership, this typically relates to cyber security training or awareness, but may include broader areas like IT training
- ❑ run a lessons-learned session with all relevant internal stakeholders (such as IT, SLT and DPO)
- ❑ write a formal incident review report, tailored to the SLT or whoever requests it, and include a timeline, impacts, lessons learned, and recommendations, with content appropriate to the setting and the nature and severity of the incident. Present the report to leadership or

your governing body if the incident was high impact or externally reportable

- ❑ implement any agreed follow-up actions - set deadlines and assign responsibility
- ❑ update your cyber security incident response and playbooks to make sure any future incidents benefit from the review

Your process:
Person responsible:

Review and testing

Cyber response plans must be accurate, practical, and aligned with statutory and sector requirements.

As part of your governance and compliance process, these actions should be reported to your trust or governing body.

Review or test	Date completed	Person responsible	Notes or actions
Scheduled annual review of cyber response plan • by SLT and DPO • with governor/trustee oversight)			
Post-incident review • an immediate debrief after an incident or exercise • a formal review within 2 weeks • lessons learned logged and integrated into the plan			

Testing feedback (from call-tree drills, table-top exercises, and technical recovery tests) used to update cyber response plan			
Contact details and escalation routes updated once per term			
Ongoing alignment to: • DfE Cyber Security Standards • NCSC guidance • UK GDPR / DPA 2018 incident reporting requirements			
Playbooks and cyber response plan cover highest risk incidents and are up to date • versions controlled and records • summary of changes maintained			

If your IT is managed by an external provider, this review may be in their remit and subject to service level agreements and contracts. Make sure you know what falls under your responsibility.

Templates

Incident recovery event recording form

This form can be used to document all key events completed throughout the stages of the Cyber Response Plan.

Adapt the form to fit your school, keeping in mind that it may need completing without IT support.

Description or reference of incident	
Date of the incident	
Date of the incident report	
Date/time incident recovery commenced	
Date recovery work was completed	
Was full recovery achieved?	

Relevant referrals

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

Actions log

Recovery tasks in order of completion	Person responsible	Completion date		Comments	Outcome
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

Email communication templates

You can use these email templates to keep staff, parents and carers, students, and the media informed throughout a cyber incident. This isn't an exhaustive list; there may be others you need to communicate with.

If your school is remaining open

Email to parents and carers

Dear parent/carer,

It appears [name of school] has been affected by [a cyber attack/serious system outage]. This has affected [some/all] of our IT systems.

This means that we currently cannot access: [list what is impacted, such as telephones, emails, servers, MIS]

We do not currently know how long it will take to restore our systems OR We expect systems will be restored by [anticipated date of restoration]

OR

We will work with the [trust / local authority], IT providers and other third parties [Department for Education / NCSC / local police constabulary] to restore functionality and normal working as soon as possible.

We are in contact with our Data Protection Officer. If required, we will report this data breach to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / GDPR.

We are taking every action to minimise disruption and data loss.

In consultation with the [trust / local authority] we have completed a risk assessment on all areas affected to address concerns about the safeguarding of our learners and staff. The school will remain open with the following changes:

[detail any changes required]

[IF APPLICABLE] I appreciate that this will cause some problems for parents and carers and apologise for any inconvenience.

We will continue to assess the situation and update you. [If possible, inform how you will update, such as via website or text message]

Yours sincerely,

Email to school staff

[School name] detected a cyber attack on [date] which has affected the following IT systems:

[provide a description of the services affected]

Following discussion with the [trust / local authority] the school will remain open with the following changes to working practice:

[detail any workarounds and/or changes]

We are in contact with our Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 and GDPR.

This incident is being investigated by the relevant authorities. If they ask you for any information as part of the on-going investigation, please provide it promptly. We have taken immediate action to mitigate data loss, limit severity, and restore systems.

You are reminded you must not make any comment or statement to the press, legal guardians or wider community about this incident or its effects. Queries should be directed to [insert staff name].

If your school is closing

Email to parents and carers

Dear parent/carer,

I am writing to inform you that it appears [school name] has been affected by [a cyberattack/serious system outage]. This has taken down the educational setting IT system. This means that we currently do not have any access to [list what is impacted, such as telephones, emails, servers, MIS]. We currently do not know how long it will take to restore our systems.

We are in contact with our Data Protection Officer. We have reported this data breach to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / GDPR.

In consultation with the [trust/local authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our learners and staff.

We have no option other than to close the educational setting to learners on [closure date]. We are currently planning that the educational setting will be open as normal on [estimated opening date].

I appreciate that this will cause some problems for you around childcare arrangements. We apologise for the inconvenience but feel that we have no option.

We will work with the [trust/local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and re-open as soon as possible.

We will continue to assess the situation and update you. [If possible, inform how you will update, such as via website or text message].

Yours sincerely,

Email to school staff

The school detected a cyber-attack on [date] which has affected the following educational setting IT systems:

[provide a description of the services affected]

Following liaison with the [trust/local authority] the educational setting will close to learners [on date OR with immediate effect].

[Detail any workarounds, changes or remote learning provisions]

The educational setting is in contact with our Data Protection Officer, and we have reported the incident to the ICO, in line with the statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The educational setting has taken immediate action to mitigate data loss; however, we are unsure when systems will be restored. Staff will be kept informed via [telephone/ email/staff noticeboard].

All staff are reminded that they must not make any comment or statement to the press, legal guardians, or wider community with regards to this incident or its effects. Queries should be directed to [insert staff name].

Media statement

[Insert school name] detected a cyber-attack on [date] which has affected the school's IT systems.

Following liaison with the [trust/local authority] the school [will remain open/is currently closed] to learners.

The school is in contact with their Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities, and the school has taken immediate remedial action to limit data loss and restore systems.

Standard guidance

Standard response

A standard staff response for serious IT incidents should reflect only information which is already freely available and has been provided by the educational setting in initial media responses.

To school staff

- the information provided should be factual and include the time and date of the incident
- staff should not speculate how long systems will take to be restored but can provide an estimate if this has been agreed
- if no restoration date has been advised, staff should merely state that work is on-going and that services will resume as soon as possible
- staff should direct further enquiries to an assigned contact/educational setting website/other pre-determined communication route

To learners

For staff responding to pupil requests for information, responses should reassure concerned learners that incidents are well prepared for, alternative arrangements are in place and that systems will be back online shortly.

Staff should address any outlandish or suggested versions of events by reiterating the facts and advising learners that this has been confirmed in letters / emails to legal guardians / carers.

Staff should not speculate or provide learners with any timescales for recovery unless the sharing of timescales has been authorised by senior staff.