YOUR PROGRAMME WORKING PACK

Make the next cyber decision clearer.

A practical record for school and trust leaders, technical colleagues and governors. Understand the service, test the response and keep unresolved decisions visible.

What you should leave with

An account of the services your school depends on, the people responsible, the evidence you have examined and the questions still needing an answer. Use the records to agree the next action and when someone will return to check it.

01 / Understand one essential school service

You can explain what the service enables, who supports it, what an interruption would affect and which question needs a decision next.

02 / Rehearse a school day without normal access

Your team has practised the handovers, identified the most consequential gap and agreed who will repair and check it.

03 / Commission cyber support with a clear result

You have a brief that defines the need, authorised scope, expected evidence, limitations and acceptance decision, with a named owner for follow-through.

How to use the pack

Begin with one service or one school-day scenario. Read the relevant guide, then complete its record with the people who understand the provision. Separate an assurance received from evidence checked, and an action agreed from work verified. The action record on page 6 and leadership review on page 9 bring the decisions together.

> Complete this blank record locally, on paper or in a PDF reader. It does not send information to School Connection. Keep it within your organisation’s approved records. Do not enter passwords, pupil information, personal incident details, network configurations or other sensitive technical material.

Official basis. Original working method.

The linked DfE and NCSC resources provide the official reference points. School Connection’s guides, rehearsal approach and records are original practical tools, not DfE-approved templates, certification or an assessment of your school. Apply current guidance to your own setting and obtain appropriately scoped specialist advice where needed. The source key on page 9 keeps the links and scope visible.

01 / ESSENTIAL SERVICE GUIDE

Understand one essential school service

Bring the school purpose, technical support, dependencies and recovery evidence into one useful account. Start with a service people recognise, then use the card to resolve what remains unclear.

When to use it: Use before a provider review, renewal, significant system change or leadership discussion. Complete it with the people responsible for the service.

Begin with work that matters to the school

Choose one function whose interruption would have a serious practical consequence: recording attendance, accessing essential safeguarding information or communicating with families. Name the function before the software. This keeps the discussion connected to people and decisions, even where several applications or organisations help deliver it.

Write what successful operation means, who relies on it and when. A boarding service may be needed after the office closes; an assessment process may become particularly time-sensitive during a defined period. This card is School Connection’s suggested planning method. It is not an asset audit or a declaration of compliance.

Put the operational and technical accounts together

Ask the school’s service owner and technical support to describe the same function. The operational owner explains the work and its consequences. Technical colleagues establish which systems and external parties make it possible. Record where their responsibilities meet, who coordinates an exception and how a deputy obtains an answer.

Follow the important dependencies

Trace the route from the authorised user to the information and action required. Ask about identity, connectivity, applications, integrations, power and external support where relevant. Identify shared dependencies that could affect other school functions. Competent technical staff should confirm the explanation; an application name alone cannot reveal the complete route.

Describe an interruption in school terms

Ask what staff would do if the normal route were unavailable. Establish the approved alternative, the person who authorises it and how essential information remains protected and sufficiently current. Record which activities would pause or operate differently. Avoid assuming that a telephone call or paper record solves every part of the service.

Leave one decision someone can carry forward

Record the evidence date, the remaining limitation, the decision required and the person with authority to make it. Agree a proportionate next action and a way to check completion. Bring significant resource or responsibility questions to leadership, with the operational consequence explained plainly.

Continue to page 3 to record the service, its dependencies and the evidence still needed.

Read the complete guide: https://schoolconnection.co.uk/cyber-resilience/guides/essential-service

02 / SERVICE AND DEPENDENCY RECORD

Start with one essential service.

Use service names and references to approved records. Record the school consequence and responsibility, without copying sensitive technical details into this pack.

School function

What work must people be able to complete, and why does it matter?

Users and hours

Who relies on it, at which sites and times, including residential or assessment periods where relevant?

Operational owner and deputy

Who owns the school function, and who acts during absence? Store personal contact details through approved arrangements.

Technical parties

Which internal teams, authority, trust services or external providers support it? Who coordinates a question across them?

Important dependencies

Which identity, connection, application, integration, power or support dependencies have competent staff confirmed?

Access responsibility

Who approves and reviews the roles permitted to use or administer it? Do not record credentials or sensitive configurations.

Consequence and priority

What would interruption affect, and who determines the operating and recovery priority?

Approved alternative

What can staff do while the usual route is unavailable? Where are the protected instructions held?

Evidence and date

What assurance, exercise or restoration evidence was examined, by whom and when?

Remaining question

What is unknown or unresolved, and what evidence would help settle it?

Next decision and owner

What action, authority or resource is needed, who owns it and when will it be reviewed?

Verification and review trigger

How will completion be checked, and which change will bring the card back for review?

03 / REHEARSAL PREPARATION

Rehearse a school day without normal access

Use a 45-minute discussion to test who receives a concern, who can decide and how essential work continues. The scenario is illustrative and uses approved exercise information throughout.

When to use it: Use while preparing or reviewing the school's response plan. This is a scheduled exercise, not a procedure to work through during a live incident.

Minutes 0 to 5: agree the people and boundaries

Appoint a facilitator and recorder. Include the senior decision-maker, IT support, attendance or office lead, designated safeguarding lead, data protection representative and communications role. Invite the examinations officer and boarding lead where relevant. One person may represent several functions where appropriate to the school's responsibilities. Agree who covers absence.

Minutes 5 to 15: introduce the lost-access morning

Read this illustrative scenario: at the start of the school day, staff cannot use their normal accounts or email. The cause and extent are unknown. Ask who receives the first report, which approved contact route still works and who coordinates the response. Staff should seek authorised support rather than investigate through improvised access.

Minutes 15 to 30: follow the school's critical handovers

Add a fictional safeguarding concern and an urgent family message. Ask the safeguarding and communications leads how authorised people obtain what they need, protect information and issue a clear instruction. Separate the known facts, the uncertainty and the decision. Identify who can approve a temporary method and how temporary records would later be reconciled.

Minutes 30 to 40: examine the return to service

The facilitator now supplies a fictional update: technical support says an important application is available again, with some questions still open. Who interprets the update, establishes what staff may resume and communicates the decision? Ask which information, permissions and checks the responsible professionals would need before accepting normal use.

Minutes 40 to 45: agree the repair and repeat

Choose the gap with the greatest practical consequence. Assign an action owner, decision-maker, completion date and a way to check the improvement. Record what worked as well as what failed. If a real concern emerges during the exercise, stop that part and use the school's actual reporting and response arrangements.

Use fictional messages and approved examples. Do not disable accounts, disconnect equipment or simulate an attack on live systems. A discussion cannot prove that backups restore, systems are clean or records are complete.

Use page 5 during or after the discussion. Record what was demonstrated, what was assumed and what remains unresolved.

Read the complete guide: https://schoolconnection.co.uk/cyber-resilience/guides/school-day-rehearsal

04 / EXERCISE OBSERVATION

Keep the discussion close to the school day.

Record decisions and observations from the agreed exercise. A discussion is not a live technical test or proof that every service can be restored.

Exercise record

Date, facilitator, recorder, participating functions and the school service examined.

Response roles

For each function, record its responsible person, deputy, authority and approved contact route. Protect personal contact details appropriately.

Exercise information

Which fictional or approved examples were used, and which activities were deliberately kept outside the exercise?

First report

Who received it, how did it reach the response lead and which communication route was demonstrated?

Attendance handover

How would the approved alternative support recording, follow-up and later reconciliation?

Safeguarding and communication

What information and authority did the relevant leads need? Which approved route was available?

Exams and residential context

Where relevant, which current instructions, external advice routes and out-of-hours responsibilities needed confirmation?

Return-to-service decision

Who would interpret the technical update and authorise and communicate permitted use?

Demonstrated and untested

What did participants actually demonstrate, what remained an assumption and what needs a separate technical test?

Improvement and verification

What will change, who owns it, when is it due and how will the relevant handover be rehearsed again?

05 / OWNED FOLLOW-THROUGH

Give each unresolved action an owner.

Choose the actions that matter after the service review or rehearsal. Give each a clear output and an agreed way to verify completion.

Action 01

What needs to change, and why?

Refer to the relevant service or observation. Keep confidential detail in the approved source record.

Responsible person or role

Who has agreed to carry this through?

Agreed due / review date

When will progress be checked?

Evidence needed and who will verify it

What would show the action has worked? Name the person who will check the result.

Action 02

What needs to change, and why?

Refer to the relevant service or observation. Keep confidential detail in the approved source record.

Responsible person or role

Who has agreed to carry this through?

Agreed due / review date

When will progress be checked?

Evidence needed and who will verify it

What would show the action has worked? Name the person who will check the result.

06 / COMMISSIONING GUIDE

Commission cyber support with a clear result

Turn an unresolved school question into work an appropriate specialist can scope, deliver and explain. Keep existing providers involved and agree how the findings will lead to action.

When to use it: Use when existing support identifies a capability or assurance gap, or before considering assessment, monitoring, incident preparation or independent verification.

Describe the question the school needs answered

Begin with the affected school function and the uncertainty. Perhaps an assurance does not cover a separately hosted service, an exercise reveals an unclear response route or nobody can show what the last restoration demonstrated. Distinguish a missing record from evidence of a technical failure. Both may justify work, but they ask different questions.

Agree authorised scope and how the teams will work together

Identify the services, sites and support relationships included. State exclusions, operating hours and any constraints around teaching, assessment or residential use. Agree which organisation can authorise access and work, how sensitive information will be handled and how changes to scope will be approved. Detailed credentials and technical access arrangements belong in protected records.

Specify evidence that will support the next decision

Match the deliverable to the commission. An assessment should explain findings, priorities and limitations. Monitoring needs defined coverage and a route from a relevant alert to someone able to act. An incident investigation needs agreed authority, information handling and interpreted conclusions. A recovery exercise should distinguish what was restored from what was only discussed.

Understand the continuing service and full commitment

Compare proposals against the same need and scope. Clarify included work, additional charges, support hours, response arrangements, school staff time and any dependency on another provider. For a continuing service, ask what happens during holidays, absence or disruption affecting the specialist itself. A monitoring subscription alone does not explain who makes the school’s decisions.

Agree acceptance and the next review before commissioning

Decide who will receive the findings, accept the deliverables and verify any corrective work. Record what evidence would justify closure and what would remain an open limitation. Establish how disagreement, an unexpected finding or a change in scope reaches someone authorised to decide. A completed visit or invoice is not automatically evidence that the intended improvement has been demonstrated.

Complete the brief on page 8 before comparing proposals. Scope, responsibilities and useful evidence should be clear to both sides.

Read the complete guide: https://schoolconnection.co.uk/cyber-resilience/guides/specialist-brief

07 / SPECIALIST COMMISSIONING BRIEF

Define the work. Agree the result.

Complete this with the school or trust team. Keep the work, expected evidence and responsibilities clear to everyone involved.

School need

Which school function and unresolved question justify the proposed work?

Existing evidence

What has already been checked, what does the current provider cover and what remains unknown?

Intended result

What answer, capability or demonstrated improvement should the commission deliver?

Authorised scope

Which services and sites are included or excluded, who can authorise the work and how will scope changes be agreed?

Operating constraints

Which teaching, assessment, residential, information-handling or access conditions must the work respect?

Coordination

Who represents the school, existing providers and specialist, and who resolves a responsibility gap?

Deliverables and limitations

Which leadership explanation and protected technical findings are required? How will exclusions and uncertainty be recorded?

Continuing response

For ongoing support, what coverage, hours, alert routing, absence and provider-disruption arrangements are agreed?

Full commitment

What charges, school time, implementation dependencies, continuing costs and exit arrangements need assessment?

Acceptance and verification

Who accepts delivery, what evidence is required and who checks that any remedy works?

Unresolved decision

Who decides when findings conflict or a material uncertainty remains?

Next review

Which action owners, dates and changes will bring the result or continuing service back for review?

08 / LEADERSHIP REVIEW AND SOURCE KEY

Explain the position. Agree the next review.

Bring together the service record, exercise observations and any proposed specialist work. This review supports a decision; it does not certify cyber resilience.

What can we explain, and what remains unresolved?

Summarise the evidence checked, the material gaps and the implications for the school day.

What happens next, who owns it and when will we return?

Record the leadership decision, the person or role responsible and the next review date.

Official reference points

Resources reviewed 4 November 2026. The official sources retain their own publication dates and scope. The working methods in this pack are School Connection’s own. Follow the programme online for the connected reporting and further source notes.

1. DfE Cyber Security Hub

Official school resources. This service card is School Connection’s own method for preparing a local conversation.

https://cyber-security-hub.education.gov.uk/

2. DfE cyber security core standard

England guidance on coordinated leadership, technical responsibilities and risk management; assess its application alongside the school’s duties.

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard

3. NCSC incident planning, response and recovery

General organisational guidance. Local operating arrangements and technical recovery need their own verification.

https://www.ncsc.gov.uk/collection/board-toolkit/principle-d-incident-planning-response-recovery/planning-your-response-to-cyber-incidents

4. DfE response-plan resources

Official templates and preparation support. Use the school’s existing plan as the basis for this original discussion exercise.

https://cyber-security-hub.education.gov.uk/create-your-cyber-response-plan

5. NCSC Exercise in a Box

Official structured exercises for further preparation. Our 45-minute scenario is separate from that service.

https://www.ncsc.gov.uk/section/exercise-in-a-box/overview