Creative Inclusion
LEARNING STUDIO

Creative Inclusion: An Independent Alternative Specialist Provision

Cyber Security and Resilience Strategy

Effective Date: July 2025
Approved by: Advisory Board August 2025
Review Date: July 2026

REVIEW SHEET

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	KAHSC Version Description	Date of Review/Revision
1	Original	July 2023
	Revised – added new link at PART A 2.2(xiv)	January 2024
2	Minor changes and additions on restoring data with links to national support mechanisms	March 2024
3	Adopted by Creative Inclusion	September 2025

CONTENTS

PART A – CYBER SECURITY AND PREVENTATIVE MEASURES 1

1. Introduction 1

1.1 Cyber Security 1

1.2 Cyber Resilience 1

1.3 Purpose of this document 1

2. Preventative strategies 2

2.1 Identify 2

2.2 Protect 2

2.3 Detect 4

PART B - CYBER RESPONSE PLAN 1

1. Introduction 1

1.1 Aims of the Cyber Response Plan 1

2. Response and recovery 1

2.1 Respond - Actions in the event of an incident 1

2.2 Recover - Restoring data and services 2

2.3 Post Incident Evaluation 3

Checklist A – Key People 1

Cyber Recovery Team 1

Server Admin Access 1

Management Information System (MIS) Admin Access 1

Checklist B - Key Roles and Responsibilities 1

Head of Provision (DSL) 1

Designated Safeguarding Lead (DSL) Role 1

Provision Business Manager 1

Data Protection Officer (DPO) 1

Chair of Advisory board 1

IT Provider 2

Teaching Staff and Teaching Assistants 2

Checklist C - Key Contacts 1

Suppliers 1

Staff Media Contact 1

Assigned Media Liaison(s): 1

Checklist D - Critical Activities - Data Assets 2

Checklist E - Backup Strategy 5

Appendix A - Incident Impact Assessment

Appendix B - Communication Templates

Appendix C - Incident Recovery Event Recording Form

Appendix D - Post Incident Evaluation

Appendix E - Risk Protection Arrangement (RPA) Cover

PART A – CYBER SECURITY AND PREVENTATIVE MEASURES

1. Introduction

1.1 Cyber Security

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorised exploitation of systems, networks, and technologies.

Cyber security should be high on the agenda for any provision with a reliance on IT and online systems. Over and above the disruption to business processes which cyber security breaches can involve, organisations that suffer cyber security breaches may face significant fines. There are also non-financial costs to be considered, like reputational damage.

1.2 Cyber Resilience

Cyber resilience is the ability of an organisation to enable business continuity by preparing for, responding to, and recovering from cyber security threats. Cyber resilience is built upon five pillars:

Identify
Firstly, provisions must have in depth knowledge of the level of security and potential risks. Therefore, the provision's essential information has to be meticulously identified and the infrastructure and information has to be evaluated, including the level of sensitivity, vulnerability and risk tolerance.

Protect
Implement the necessary protection measures. Protection measures for critical infrastructures and services have to be developed and implemented, with the aim of mitigating or reducing the level of vulnerability.

Detect
Appropriate actions must be implemented in order to rapidly identify an attack, evaluate the affected systems and guarantee a timely response. Furthermore, during this stage, the network must be continuously monitored in order to identify any other indicators related to that attack.

Respond
Provisions need a response plan, headed by a team of people with specifically identified functions and responsibilities.

Recover
This phase involves developing and implementing systems and plans to restore data and services that may have been affected during a cyber-attack.

1.3 Purpose of this document

This document is purposely divided into two parts. **Part A** is designed to help the provision to focus on the arrangements and precautions required in order to develop and maintain an appropriate level of cyber security within its IT infrastructure and its day to day operations. Accordingly, Part A concentrates on the 'Identify', 'Protect' and 'Detect' pillars of cyber resilience.

Part B of this document takes the form of a Cyber Response Plan, enabling the provision to consider the arrangements we will need to put in place to successfully ensure that the 'Respond' and 'Recover' pillars of cyber resilience are effectively addressed.

The document has been designed this way so that Part B can be utilised independently of Part A in the event of a cyber-attack on the provision. Part B contains a number of templates for forms and aide- mémoires which can be utilised by the Cyber Recovery Team to help manage the provision's response to a cyber-attack.

2. Preventative strategies

It is vital that we understand our vulnerabilities and regularly review our existing defences and take the necessary steps to protect our networks. As well as having a current and cohesive Cyber Response Plan in place, there are several measures that we can implement to help to improve our IT security and mitigate the risk of a cyber-attack. These measures fall under the 'Identify, Protect and Detect' pillars of effective cyber resilience and are outlined below.

2.1 Identify

In order to identify our vulnerabilities, we must understand not only the hardware and software components which make up our IT infrastructure and networks, but also the types of threats that these components may be exposed to. In order to achieve this we will, in conjunction with our IT provider(s), implement the following measures:

i. Maintain an up to date inventory of **all** IT hardware and software utilised by the provision in our day to day operations.
ii. Maintain an up to date inventory of **all** information/data sets to which the provision has access (see Checklist D). Include an evaluation of the level of sensitivity, vulnerability and risk tolerance associated with individual information/data sets and understand which are critical to business continuity in the event of a cyber-attack.
iii. Regularly review our IT Security Policy and Data Protection Policy and procedures to ensure they remain current and stay abreast of developments and emerging threats in relation to IT security.
iv. Assess the provision's current security measures against Cyber Essentials requirements such as firewall rules, secure device configuration, security update management, user access control and malware protection. Cyber Essentials is a government-backed baseline standard, which we will strive towards achieving wherever possible.

2.2 Protect

Once we properly understand the scope of our IT infrastructure, we can ensure that appropriate protection measures are developed and implemented with the aim of mitigating or reducing our level of vulnerability. In order to achieve this we will follow the Cyber security standards guidance included in 'meeting digital and technology standards in provisions and colleges' set out by the Department for Education (DfE) and ensure, in conjunction with our IT partner(s) where appropriate, that the following safeguards are in place:

i. All devices on every provision network are protected with a properly configured boundary or software firewall.

ii. All devices that can access the provision's network (including where provisions allow learners to access the network via their own device) are known and recorded with their security features enabled, correctly configured and kept up to date.

iii. Account holders only have the access they require to perform their role and will be authenticated to access data and services.

iv. Account holders with access to personal or sensitive operational data and functions are protected by multi-factor authentication (a method of confirming a user's identity by using a combination of two or more different factors).

v. Anti-malware software is used to protect all devices in the network, including cloud-based networks (see National Cyber Security Centre (NCSC) advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks).

vi. An administrator will check the security of all applications downloaded onto a network.

vii. All online devices and software must be licensed for use and will be patched with the latest security updates.

viii. We will have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 of which will be off-site and at least 1 will be offline at any given time. Help and guidance on backing up is available from the NCSC. Backups will be tested regularly to ensure that services can be restored, and data recovered from them.

ix. Our provision Emergency Plan will include a regularly tested contingency plan in response to a cyber-attack – our 'Cyber Response Plan' – designed to be implemented by a team of people with specifically identified functions and responsibilities in the event of a cyber-attack. We will communicate the Cyber Response Plan to all those who are likely to be affected and will inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.

x. We will ensure that the measures which we have in place comply with the requirements of our insurers.

xi. We will report any suspicious cyber incident to the relevant agency. This may include Action Fraud, the DfE sector cyber team, the Information Commissioners Office (ICO), and the NCSC, depending upon the type and seriousness of the incident.

xii. We will conduct a Data Protection Impact Assessment by statute for personal data we hold as required by the UK General Data Protection Regulation (UK GDPR).

xiii. All employees or Advisory board members who have access to the provision's IT system will undertake NCSC Cyber Security Training. Upon completion, a certificate will be downloaded by each person, a copy of which will be held centrally by the provision. In the event of a claim a copy of this certificate may be required as evidence.

xiv. We will make use of the extensive range of free practical resources available on the SWGFL and NCSC website to help improve Cyber Security within our provision. These include the following topics:

- CyberSecure Check for Provisions – a free cyber security tool.
- Cyber security in provisions: questions for advisory board members and trustees
- Cyber security toolkit for boards
- Cyber security training for provision staff
- Early Years practitioners: using cyber security to protect your settings
- Resources for provisions

xv. We can also access a range of support from the North West Cyber Resilience Centre (NWCRC). They offer a range of paid for services including security awareness training and website vulnerability assessments but will also provide free advice to provisions.

xvi. We will ensure all users have read the relevant Policies and signed IT acceptable use agreements for provision devices.

xvii. We will make staff aware that if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the Police.

2.3 Detect

Early detection of cyber threats can help to significantly mitigate the impact upon our IT infrastructure and help preserve the continuity of business functions through the timely deployment of counter measures and our response plan. The following measures will help us to identify threats at an early stage and initiate a timely response:

i. Installation and regular updating of anti-malware software will help to detect and mitigate the effects of a cyber-attack.

ii. Delivery of cyber security training to all staff and Advisory board members will serve to heighten their awareness of cyber threats and help them to identify and understand the importance of reporting potential security breaches immediately.

iii. We will use the NCSC Exercise in a Box toolkit to help our staff understand what a cyber-attack might look like and to test our response plans to identify any weaknesses.

iv. We will register with Police CyberAlarm. Registering will connect our provision with the local police cyber protect team and should allow a cyber-alarm software tool to be installed for free to monitor cyber activity. The tool, when installed, will record traffic on the network without risk to personal data.

v. As soon as an attack is detected we will:

- work with our IT partner(s) to evaluate the affected system(s) and continuously monitor them in order to identify any other indicators related to the attack.
- Initiate our Cyber Response Plan and convene our cyber recovery team to ensure that we effectively deliver the 'Respond' and 'Recover' pillars of our cyber resilience strategy. **SEE PART B – CYBER RESPONSE PLAN**

PART B - CYBER RESPONSE PLAN

1. Introduction

This Cyber Response Plan has been developed as part of our overall Emergency Plan which is required in order to ensure that we maintain a minimum level of functionality to safeguard learners and staff and to restore the provision back to an operational standard following a cyber-attack. The Cyber Response Plan will cover all essential and critical IT infrastructure, systems, and networks.

1.1 Aims of the Cyber Response Plan

The aim of our Cyber Response Plan is to ensure that we can effectively deliver the 'Respond' and 'Recover' pillars of our cyber security strategy in the event of a cyber-attack. The plan will enable provision staff and key stakeholders to have a clear understanding of who should be contacted, and the actions necessary to minimise disruption and facilitate a recovery to normal business functioning.

Within the Plan we have considered who will be involved in the Cyber Recovery Team, the key roles and responsibilities of staff, what data assets are critical and how long we would be able to function without each one. We have also established plans for internal and external communications and have thought about how we would access registers and staff and learner contact details. This will allow the provision to:

- ensure immediate and appropriate action is taken in the event of an IT incident;
- enable prompt internal reporting and recording of incidents;
- have immediate access to all relevant contact details (including backup services and IT technical support staff);
- maintain the welfare of learners and staff;
- minimise disruption to the functioning of the provision;
- ensure that the provision responds in a consistent and effective manner in order to reduce confusion and reactivity;
- restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the provision which are unaffected;
- report cyber incidents to the relevant authorities.

2. Response and recovery

Speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.

2.1 Respond - Actions in the event of an incident

Where we suspect, or are informed by others, that we have been the victim of a ransomware or other cyber incident, we will take the following steps immediately:

1. Convene the Cyber Recovery Team.
2. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.
3. Assess and document the scope of the incident using the Incident Impact Assessment at Appendix A to identify which key functions are operational/which are affected.
4. Start the Actions Log to record actions taken.

5. Contact the RPA Cyber Emergency Assistance 24hr helpline:
    - By telephone: 0800 368 6378 or by email: RPAresponse@CyberClan.com;
    - We will receive a guaranteed response within 15 minutes;
    - Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible;
    - Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including forensic investigation services and support in bringing IT operations securely back up and running.
6. In the event of a suspected cyber-attack, our IT partner(s) will be asked to isolate devices from the network.
7. In order to assist subsequent data recovery, if damage to a computer or back up material is suspected, we will ensure that staff **do not:**
    - turn off electrical power to any computer.
    - try to run any hard drive, back up disc or tape to try to retrieve data.
    - tamper with or move damaged computers, discs or tapes.
8. Make a decision as to the safety of the provision remaining open.
    - *This will be in liaison with relevant Local Authority Support Services/Trust*
9. Identify legal obligations and any required statutory reporting e.g. criminal acts/reports to the Information Commissioner's Office in the event of a data breach.
    - *This may involve the provision's Data Protection Officer and the Police*
10. Execute the communication strategy which should include a media/press release if applicable.
    - *Communications with staff, advisory board member and parents/learners should follow in that order, prior to the media release.*
11. Contact the local Police via the Action Fraud website or call **0300 123 2040**.
12. Contact our Data Protection Officer.

2.2 Recover - Restoring data and services

When we are sure that the initial threat has been contained and either quarantined or removed, we will begin the process of restoring normality to our business functions as far as practicable. The National Cyber Security Centre have published a one page step-by-step guide to recovering online accounts. To help facilitate the restoration, we will undertake the following actions:

1. Continue to liaise with insurance provider for advice and guidance.
2. Check email accounts for unwanted forwarding rules.
3. Contact any account contacts to let them know that the email or social media account has been hacked and suggest they treat any recent emails or other messages sent from the account with suspicion.
4. Change passwords for any account that has been hacked and also for any accounts that use the same password.
5. Agree a process with our IT partner(s) for safely restoring any systems/databases which have been affected.
6. Maintain the Actions Log to record recovery steps and monitor progress.

7. Maintain a dialogue with our IT partner(s) to estimate the recovery time and likely impact.
8. If money has been lost, inform the Bank and report it as a crime to Action Fraud.
9. Keep stakeholders informed of progress and likely timescales.

2.3 Post Incident Evaluation

Upon completion of the 'Respond' and 'Recover' processes we will evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix D and review the Cyber Response Plan accordingly.

In particular we will consider if there was any information/data which would have significantly helped our response, but which was difficult or impossible to obtain. We will plan to gather this information/data ahead of any future attacks.

We will communicate the evaluation findings to staff and key stakeholders to ensure that relevant learning is disseminated appropriately.

We will ensure that the Cyber Response Plan is kept up to date with new suppliers, new contact details, and any changes to policy as appropriate.

Checklist A – Key People

Cyber Recovery Team

In the event of this plan having to be initiated, the personnel named below will form the Cyber Recovery Team and take control of the following:

	Name	Role in Provision	Contact Details
Recovery Team Leader	Joanne Vance	Head of Provision	07398 824988
Data Management			
IT Restore / Recover			
Site Security			
Public Relations			
Communications			
Resources / Supplies			
Facilities Management			

Server Admin Access

Please detail all the people with administrative access to the server.

Role	Name	Contact Details
Head of Provision	Joanne Vance	07398 824988
Business Manager		
IT Support Technician		
Third Party IT Provider		

Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Head of Provision	Joanne Vance	07398 824988
Business Manager		
MIS Provider	LearnTrek	
Data Manager		

In the event of a cyber incident, it may be helpful to consider how you would access the following:

- Registers
- Staff / Learner contact details
- Current Child Protection Concerns

Checklist B - Key Roles and Responsibilities

Every provision is unique and the structure and staffing levels will determine who will be assigned which task. We have used the following checklist to assist us to assign roles and responsibilities. This is not an exhaustive or a definitive list.

Head of Provision (DSL)

- ☐ Seeks clarification from person notifying incident.
- ☐ Sets up and maintains an incident log, including dates / times and actions.
- ☐ Convenes the Cyber Recovery Team (CRT) to inform of incident and enact the plan.
- ☐ Liaises with the Chair of Advisory board members.
- ☐ Liaises with the provision Data Protection Officer.
- ☐ Convenes and informs staff, advising them to follow the 'script' when discussing the incident.
- ☐ Prepares relevant statements / letters for the media, parents / learners.
- ☐ Liaises with Provision Business Manager to contact parents, if required, as necessary.
- ☐ Ensures site access for external IT staff.

Designated Safeguarding Lead (DSL) Role

- ☐ Seeks clarification as to whether there is a safeguarding aspect to the incident.
- ☐ Considers whether a referral to Cyber Protect Officers / Early Help / Safeguarding Hub/MACH is required.

Business Manager

- ☐ Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
- ☐ Ensures office staff understand the standard response and knows who the media contact within provision is.
- ☐ Contacts relevant external agencies – RPA or Insurance Provider Emergency Assistance / IT services / technical support staff.
- ☐ Manages the communications, website / texts to parents / provision emails.
- ☐ Assesses whether payroll or HR functions are affected and considers if additional support is required.

Data Protection Officer (DPO)

- ☐ Supports the provision, using the provision data map and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- ☐ Liaises with the Head of Provision / Chair of Advisory board members and determines if a report to the ICO is necessary.
- ☐ Advises on the appropriateness of any plans for temporary access / systems.

Chair of Advisory board

- ☐ Supports the Head of Provision throughout the process and ensure decisions are based on sound judgement and relevant advice.
- ☐ Understands there may be a need to make additional funds available – have a process to approve this.
- ☐ Ensures all Advisory board members are aware of the situation and are advised not to comment to third parties / the media.

- ☐ Reviews the response after the incident to consider changes to working practices or provision policy.

IT Provider

Depending upon whether the provision has internal or outsourced IT provision, the roles for IT Co-ordinators and technical support staff will differ.

- ☐ Verifies the most recent and successful backup.
- ☐ Liaises with the RPA or Insurance Provider 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 Head of Provision 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 learners, staying within agreed learner standard response
- ☐ Records any relevant information which learners may provide.
- ☐ Ensures any temporary procedures for data storage / IT access are followed.

Checklist C - Key Contacts

Suppliers

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection		
Backup Provider		
Telecom Provider		
Website Host		
Electricity Supplier		
Burglar Alarm		
Text Messaging System		
Action Fraud	**0300 123 2040**	
Local Constabulary	**101**	
Legal Representative		

Staff Media Contact

Assigned staff will co-ordinate with the media, working to guidelines that have been previously approved for dealing with post-disaster communications.

The staff media contact should only provide verified facts. It is likely that verifying details will take some time and stating, “I don’t know at this stage”, is a perfectly acceptable response.

It is likely the following basic questions will form the basis of information requests:

- What happened?
- How did it happen?
- What are you going to do about it?

Staff who have not been delegated responsibility for media communications **should not respond** to requests for information and should refer callers or media representatives to assigned staff.

Assigned Media Liaison(s):

Name:		**Role:**	Head of Provision
Name:		**Role:**	Chair of Advisory board

Checklist D - Critical Activities - Data Assets

List all the data assets your provision has access to and decide which are critical and how long you would be able to function without each one. This could be a matter of a few hours or a matter of a day, a week or even a month.

Complete the required column with the timescale you believe is necessary for recovery. You may find it helpful to refer to your Inventory / Data Map.

Assign: 4 hours / 12 hours / 24 hours / 48 hours / 72 hours / 1 week / 2 weeks / 3 weeks / 1 month

Also decide if there are any temporary workarounds or if outsourcing is possible. It is useful to consider the cost of any additional resources which may be required in an emergency situation.

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No) or how
Leadership and Management	Access to Head of Provision's email address	timescale	Yes
	Minutes of SLT meetings and agendas		
	Head's reports to advisory board members (past and present)		
	Key stage, departmental and class information		
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns	4 hours??	E.g. Revert to paper system if electronic system is down or inaccessible
	Attendance registers		As above
	Class groups / teaching groups, and staff timetables		
	Referral information / outside agency / TAFs		
	Child protection records		
	Looked After Children (LAC) records / PEPs		
	Learner Premium learners and funding allocations		
	Pastoral records and welfare information		
Medical	Access to medical conditions information		
	Administration of Medicines Record		
	First Aid / Accident Logs		
Teaching	Schemes of work, lesson plans and objectives		

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No) or how
	Seating plans		
	Teaching resources, such as worksheets		
	Learning platform / online homework platform		
	Curriculum learning apps and online resources		
	CPD / staff training records		
	Learner reports and parental communications		
SEND Data	SEND List and records of provision		
	Accessibility tools		
	Access arrangements and adjustments		
	IEPs / EHCPs / GRIPS		
Conduct and Behaviour	Reward system records, including house points or conduct points		
	Behaviour system records, including negative behaviour points		
	Sanctions		
	Exclusion records, past and current		
	Behavioural observations / staff notes and incident records		
Assessment and Exams	Exam entries and controlled assessments		
	Targets, assessment and tracking data		
	Baseline and prior attainment records		
	Exam timetables and cover provision		
	Exam results		
Governance	Provision development plans		
	Policies and procedures		
	Advisory board members' meeting dates / calendar		
	Board member attendance and training records		
	Advisory board members' minutes and agendas		
Administration	Admissions information		
	Provision to provision transfers		
	Transition information		
	Contact details of learners and parents		
	Access to absence reporting systems		

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No) or how
	Provision diary of appointments / meetings		
	Learner timetables		
	Letters to parents / newsletters		
	Extra-curricular activity timetable and contacts for providers		
	Census records and statutory return data		
Human Resources	Payroll systems		
	Staff attendance, absences, and reporting facilities		
	Disciplinary / grievance records		
	Staff timetables and any cover arrangements		
	Contact details of staff		
Office Management	Photocopying / printing provision		
	Telecoms - provision phones and access to answerphone messages		
	Email - access to provision email systems		
	Provision website and any website chat functions / contact forms		
	Social media accounts (Facebook / Twitter)		
	Management Information System (MIS)		
	Provision text messaging system		
	Provision payments system (for parents)		
	Financial Management System - access for orders / purchases		
Site Management	Visitor sign in / 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	Contact information for catering staff		
	Supplier contact details		
	Payment records for food & drink		

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No) or how
	Special dietary requirements / allergies		
	Stock taking and orders		

Checklist E - Backup Strategy

Provision Process	Backup Type (include on-site/off-site)	Frequency
Main File Server	Off-site / Name of IT provider	
Provision MIS	Via LearnTrek	
Cloud Services	Are they automatically backed up or do you have to specify or do manually.	
Third Party Applications / Software	Reading schemes or maths schemes, CPOMS. PDF reader, your security software (if not organised by your IT provider) Zoom etc. if you use any of these - all these are third party applications. The point of all this is so that in the event you are wiped out, you will have a list of all the applications you had in order to restore them without having to remember what you had.	
Email Server	Off-site/Name of IT provider	
Curriculum Files	If these are on your current server, then it will be backed up by your IT provider and the frequency will be the same as above.	
Teaching Staff Devices		
Administration Files		
Finance / Purchasing		
HR / Personnel Records		
Inventory	Again, this will probably be on your server, but might be backed up to a pen drive - if so, how often is it backed up.	
Facilities Management / Bookings	Will not applicable if you don't hire out your premises on a regular basis or take bookings for anything much.	
Website	Is your website backed up by someone other than your IT provider, if so, it will be your provider for the website.	
USBs / portable drives		

Incident Impact Assessment

Understanding the type and severity of an incident allows you to determine how urgent your response is. It also enables you ensure that the correct people are involved from the outset. Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

Operational	No Impact	There is no noticeable impact on the provision'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 provision 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 provision can no longer provide any critical services to users. It is likely the provision 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 provision 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 provision.
	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.

Communication Templates

1. Provision Open (notification to parent/carer)

Dear Parent/Carer,

I am writing to inform you that it appears the provision has been a victim of [a cyber-attack / serious system outage]. This has taken down [some / all] of the provision IT systems. This means that we currently do not have any access to [telephones / emails / server / MIS etc.]. At present we have no indication of how long it will take to restore our systems. [OR it is anticipated it may take XXXX to restore these systems].

We are in liaison with our provision Data Protection Officer and, if required, this data breach will be reported to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / UK GDPR. Every action has been taken to minimise disruption and data loss.

The provision will be working with the [Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and normal working as soon as possible.

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. The provision will remain open with the following changes [detail any changes required].

I appreciate that this will cause some problems for parents/carers with regards to provision communications and apologise for any inconvenience.

We will continue to assess the situation and update parents/carers as necessary. [If possible, inform how you will update i.e. via website/text message].

Yours sincerely,

2. Provision Closure (notification to parent/carer)

Dear Parent/Carer,

I am writing to inform you that it appears the provision has been a victim of [a cyber-attack / serious system outage]. This has taken down the provision IT system. This means that we currently do not have any access to [telephones / emails / server / MIS etc.]. At present we have no indication of how long it will take to restore our systems.

We are in liaison with our provision Data Protection Officer and this data breach has been reported to the Information Commissioners Office (ICO) in line with the requirements of the Data Protection Act 2018 / UK 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.

I feel that we have no option other than to close the provision to learners on [XXXX]. We are currently planning that the provision will be open as normal on [XXXX].

I appreciate that this will cause some problems for parents/carers with regards to childcare arrangements and apologise for any inconvenience but feel that we have no option other than to take this course of action.

The provision will be working 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 parents / carers as necessary. [If possible, inform how you will update i.e. via website / text message].

Yours sincerely,

3. Staff Statement (Provision Open)

The provision detected a cyber-attack on [date] which has affected the following provision IT systems: [Provide a description of the services affected].

Following liaison with the [Trust / LA] the provision will remain open with the following changes to working practice:

[Detail any workarounds / changes]

The provision is 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 / UK 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 provision has taken immediate action to mitigate data loss, limit severity, and restore systems.

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

4. Staff Statement (Provision Closed)

The provision detected a cyber-attack on [date] which has affected the following provision IT systems: [Provide a description of the services affected].

Following liaison with the [LA] the provision will close to learners [on DATE or with immediate effect].

[Detail staff expectations and any workarounds / changes or remote learning provision].

The provision 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 / UK 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 provision 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, parents, or wider community with regards to this incident or its effects. Queries should be directed to [Insert staff name].

5. Media Statement

[Inset provision name] detected a cyber-attack on [date] which has affected the provision IT systems. Following liaison with the [LA] the provision [will remain open / is currently closed] to learners.

The provision 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 / UK GDPR.

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

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

Standard Response

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 practically possible.

Staff should direct further enquiries to an assigned contact / provision website / other pre-determined communication route.

Standard Response for Learners

For staff responding to learner 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 parents / carers.

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

Incident Recovery Event Recording Form

This form can be used to record all key events completed whilst following the stages of the Cyber Response Plan.

1. Incident Details

Description or reference of incident:	e.g. malware, DoS, phishing, data breach, targeted attack, accidental/malicious insider action, unauthorised access etc.
Date of the incident:	
Date of the incident report:	
Date/time incident recovery commenced:	
Date recovery work was completed:	
Was full recovery achieved?	

2. Relevant Referrals

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

3. Actions Log

Recovery Tasks (*In order of completion*)	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

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		
Enactment of the Action plan		
Co-ordination of the Cyber 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:		

Risk Protection Arrangement (RPA) 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."

RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident, we will 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 we take the necessary steps to protect our networks from cyber-attacks and have the ability to restore systems and recover data from backups. We will ask our [IT team/external IT provider] to ensure the following:

   a) Backup 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 Advisory board members who have access to the provision's IT system must undertake NCSC Cyber Security Training by 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. The RPA provides a template which can be used to draft a provision-specific plan if one is not already available. 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.