# *"Your Organisation's"*

# Cyber Incident Response Plan

## APPENDICES

Within this plan are several appendices to use.

Appendix A - Contacts Directory
Appendix B - Action Card for a manager receiving a report of cyber incident
Appendix C - Incident Log to record initial actions
Appendix D - Strategic Decision Log
Appendix E - Advice to give to staff reporting a Cyber Security Incident
Appendix F - Tactical Manager Action Card
Appendix G - Strategic Manager Action Card
Appendix H - Lessons Learned Report
Appendix I – Cyber Action Guide
Appendix J - Wall Sign
Appendix K - Device out of action sign
Appendix L – Version Control Information

# CYBER INCIDENT RESPONSE PLAN

This template has been developed to help organisations respond effectively to cyber incidents and disruption. It is designed for small businesses, charities, community organisations, sports clubs, and professional services firms.

This plan should be used alongside business continuity plans, data protection procedures, IT disaster recovery plans, and cyber essentials controls.

## HOW TO USE THIS TEMPLATE

**You** are free to use, adapt, and build upon this material, but you may not use it for commercial purposes. This was developed to support organisations in improving cyber resilience and incident preparedness.

**We** suggest reviewing the pack and editing names and numbers where necessary, before you distribute to your organisation. **Consider** printing to help staff with a clear reporting procedure in the beginning of any incident.

**Use the** checklist to provide a prompt response that will limit the damage of any attack, whilst communicating effectively through your channels to keep suppliers, customers, and staff informed. The checklist will help to calmly guide a response through a time of heightened stress and confusion.

## REPORTING INCIDENTS

Business or charity suffering a live cyber attack? Contact Report Fraud on 0300 123 2040.

If you think it's suspicious, or a scam, report it…

- Forward Emails to report@phishing.gov.uk
- Report Websites at ncsc.gov.uk/section/about-this-website/report-scam-website
- Forward Texts or Calls to 7726
- If you have disclosed banking details or authorised a payment, call 159 immediately.
- Lost money or been hacked reportfraud.police.uk
- Emergency situations 999 if immediate danger to life/someone using/threatening violence
- Pass useful information to crime stoppers 0800 555111



# CYBER SECURITY CONSEQUENCES

You should keep your organisation's computer systems and data safe and functional whilst maintaining a service provision. There are many ways in which cyber security incidents can negatively impact your organisation.

The main impacts can be broadly categorised into 5 areas:

1. **Physical/Digital** - infection of your computer systems and that of your supply chain, or loss of personal or private information leading to regulatory consequences.

2. **Economic** - the asset is compromised and must be replaced or repaired incurring a financial cost.

3. **Psychological** - confusion and disarray while the organisation regroups to work around the attack.

4. **Reputational** - unfavourable scrutiny, loss of confidence and goodwill or business.

5. **Social/societal** - negative changes in public perception and an adverse change in how the public engages with the organisation.

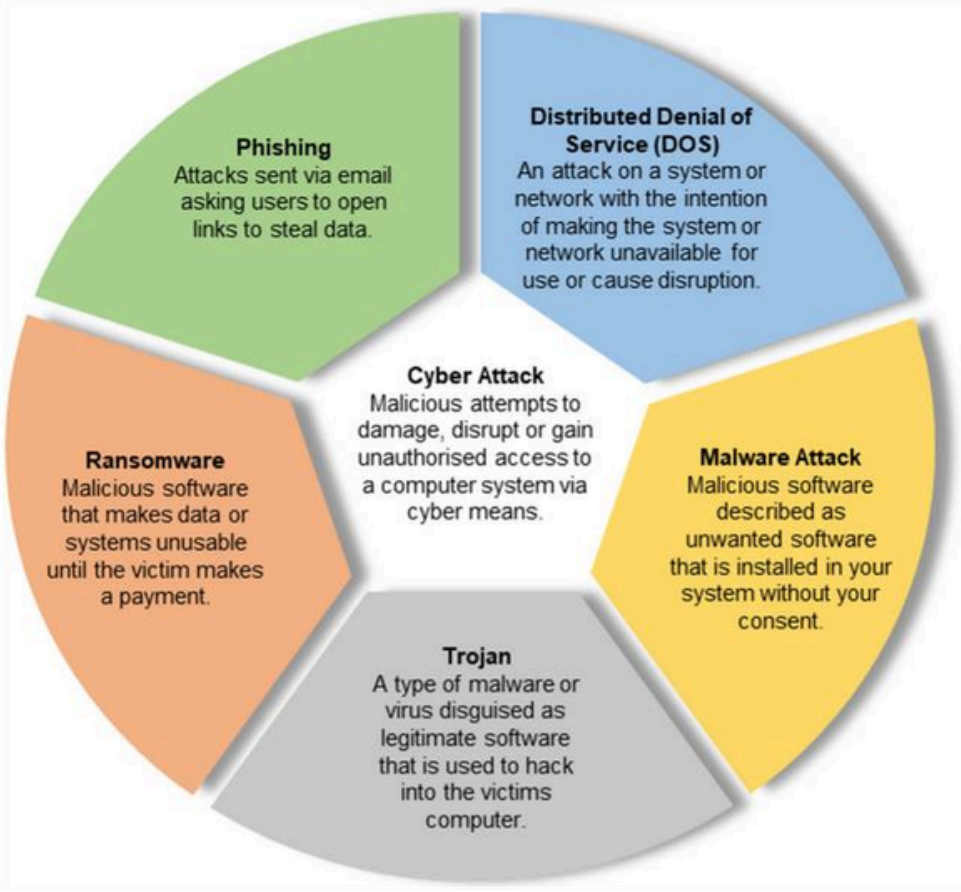
## IT FAILURES OR CYBER ATTACKS?

Cyber attacks may initially present as computer system failures, glitches, or smaller losses of IT service.

Any member of staff may report or escalate a suspected cyber incident. Formal declaration should be made by the most appropriate responsible person available.

These plans contain initial actions to address IT loss, including actions to isolate potentially compromised computers and reporting of the incident to the person responsible for IT.

**All plans should be held in paper copy as well as electronically, so they are independent of IT access and easily found when required.**



# WHAT IS A CYBER SECURITY INCIDENT?

The National Cyber Security Centre (NCSC) defines a cyber security incident as:

- A breach of a computer system's security policy to affect its integrity or availability.
- The unauthorised access or attempted access to a computer system.

## Activities commonly recognised as security policy breaches are:

- Attempts to gain unauthorised access to a computer system and/or to data.
- The unauthorised use of computer systems and/or data.
- Modification of a computer system's firmware, software, or hardware without the computer system owner's consent.
- Malicious disruption and/or denial of service.

The attack methodology for a cyber security incident varies greatly, as will the associated response.

The scale of a cyber security incident will not always be determined or obvious from the outset.

The nature of cyber-attacks evolves very quickly, some typical cyber-attack methods are outlined below.

## Current Examples:

- Business Email Compromise
- MFA fatigue or repeated approval requests
- Unauthorised access to Microsoft 365 or Google Workspace
- QR code phishing
- Supplier or supply chain compromise
- Deepfake voice or video-enabled fraud
- Malicious forwarding rules in email accounts
- Cloud account compromise
- Data theft before ransomware deployment



# CYBER SECURITY INCIDENT ASSESSMENT PROCESS

Cyber security incidents should be assessed for severity at an early stage. External organisations may also provide information or advice that helps assess the nature, scale and potential impact of the incident.

It is important to understand how the assessment process works so you know when to activate your Cyber Security Incident Plan. Once a cyber security incident is declared the following roles overleaf should be established to deal effectively with the incident.

The Incident Lead should:

- Establish a Cyber Incident Response Team.
- Confirm the severity level of the incident.
- Maintain an incident log.
- Allocate clear responsibilities.
- Schedule regular situation updates.
- Ensure communications remain accurate and consistent.
- Support recovery and restoration activities.
- Capture lessons learned following resolution.

Any member of staff may report or escalate a suspected cyber incident. Formal declaration of a cyber incident should be made by the most appropriate responsible person available, normally:

- Business Owner
- Senior Leader
- IT Provider / MSP
- Information Security Lead
- Incident Lead

## EARLY HELP

Appendix J is a template wall poster to use in offices to assist staff in the reporting of a cyber incident and providing early guidance. Consider editing and affixing these in common areas.

## ALERT STANDBY AND ACTIVATION TRIGGERS

The notification of a cyber security incident may come from several possible sources:

- Self-identification by IT, Information Security, or other internal user.
- Notification via the national structures of the National Cyber Security Centre (NCSC)
- or intelligence from another partner organisation.



## TASKS

The initial responder should refer to Appendix B – Action Card for a manager receiving a report of cyber incident.

| Role | Responsibility |
|---|---|
| **Incident Lead** | Overall coordination of the incident. Chairs meetings, allocates actions, monitors progress and ensures the response remains focused on recovery and business priorities. |
| **Business Owner / Chief Executive / Senior Leader** | Sets overall strategy and priorities. Makes key decisions regarding service continuity, communications, regulatory reporting and expenditure. |
| **IT Lead / MSP** | Leads the technical investigation, containment, eradication and recovery of affected systems. Preserves technical evidence where required. |
| **Information Security Lead** | Assesses cyber risks, advises on containment measures, supports investigation and provides security guidance throughout the incident. |
| **Data Protection Officer (DPO where appointed)** | Assesses potential impact on personal data, determines reporting requirements and coordinates any notifications to the Information Commissioner's Office (ICO). |
| **Communications Lead** | Coordinates communications with staff, customers, suppliers, partners and media. Ensures messaging is accurate, timely and approved. |
| **Business Continuity Lead** | Coordinates continuity arrangements to maintain critical services and minimise disruption whilst systems are recovered. |
| **Finance Lead** | Assesses financial impact, authorises emergency expenditure and liaises with banks where fraud or financial compromise is suspected. |
| **Human Resources Lead** | Supports staff welfare, manages internal communications and assists where employee accounts, devices or insider threats are involved. |
| **Legal Adviser** | Provides advice on legal obligations, contractual issues, regulatory requirements and evidence preservation. |
| **Cyber Insurance Provider** | Provides incident support, specialist response services and guidance in accordance with policy conditions. |
| **External Specialists** | May include forensic investigators, incident response companies, legal advisers, PR consultants or sector specialists depending on the nature of the incident. |

# INCIDENT SEVERITY LEVELS

Cyber incidents should be assessed early and reviewed regularly. Severity may increase or decrease as more information becomes available.

Severity should reflect the actual or potential impact on the organisation, not solely the number of affected systems or users.

**Severity 1: Critical Incident**

A critical incident is likely to cause major disruption, serious financial loss, significant data compromise or major reputational damage. Examples:



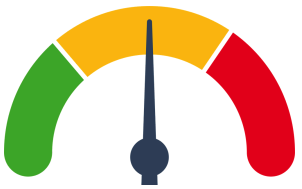
- Ransomware affecting multiple systems.
- Loss of access to core business systems.
- Confirmed unauthorised access to sensitive data.
- Fraud involving significant financial loss.
- Incident attracting media, regulator or law enforcement interest.
- Major supplier or customer impact.

Immediate actions:

- Activate the Cyber Incident Response Team.
- Notify senior leadership / the business owner immediately.
- Consider activating business continuity arrangements.
- Notify your cyber insurer promptly, where applicable.
- Consider external legal / PR / forensic / law enforcement support.
- Assess whether ICO / sector-specific regulator notification is required.
- Start an incident log.

**Severity 2: Significant Incident**

A significant incident has a noticeable impact but is currently limited in scale. Examples:



- A single department affected.
- One or more user accounts compromised.
- Suspected but unconfirmed data exposure.
- Malware detected on a small number of devices.
- Business email compromise attempt.
- Supplier compromise with possible impact.

Immediate actions:

- Notify IT support or your managed service provider (MSP).
- Notify the responsible senior manager.
- Start an incident log.
- Assess whether escalation to Severity 1 is required.
- Monitor for further spread or indicators of compromise.

**Severity 3: Minor Incident**

A minor incident appears isolated and has limited immediate impact. Examples:



- Suspicious email reported but not clicked.
- Single device showing unusual behaviour.
- Failed login alerts.
- Suspected scam contact.
- Lost device with low risk and suitable protections in place.

Immediate actions:

- Record the incident.
- Notify IT support or the responsible person.
- Preserve relevant evidence.
- Review whether further action is required.
- Use the incident as an opportunity to improve staff awareness.

**RANSOMWARE CONSIDERATIONS**

**Do not rush to pay a ransom**

**Payment does not guarantee recovery**

# Communications

Effective communication is critical during a cyber security incident. If your organisation, a supplier, or another organisation within your supply chain is affected, normal communication methods may become unavailable or untrusted.

A successful cyber attack can impact email, Microsoft Teams, Voice over Internet Protocol (VoIP) telephony, intranet services, websites and internet connectivity. This can significantly affect your ability to coordinate internally and communicate with customers, suppliers, regulators and other stakeholders.

Organisations should have a resilient communications plan that identifies alternative methods of communication should primary systems fail. Consider including:

- Offline contact lists for key personnel and critical suppliers.
- Dedicated or alternative mobile telephone numbers.
- A pre-approved out-of-band communication method (such as WhatsApp or Signal) for the Incident Response Team, where this has been risk assessed and authorised.
- Alternative conference call facilities or meeting locations.
- A nominated spokesperson responsible for all external communications.
- Pre-prepared internal and external holding statements.

Where critical suppliers provide key business services, understand how they will communicate with you if they experience a cyber security incident and their normal communication channels are unavailable.

## Internal Communications

Staff should:

- Use only approved communication channels.
- Report anything unusual immediately.
- Avoid discussing the incident externally or on social media.
- Follow instructions from the Incident Response Team.
- Await verified updates rather than relying on rumours or speculation.



## External Communications

Communications with customers, suppliers, regulators, insurers and the media should be coordinated through a nominated spokesperson or Incident Management Team.  Communications should always:

- Be timely, accurate and transparent.
- Clearly distinguish confirmed facts from ongoing investigations.
- Never speculate on the cause, attribution or impact of the incident.
- Provide regular updates, even if there is little new information.
- Adapt holding statements to the confirmed facts and avoid misleading descriptions of the incident.

## Holding Statements

### Internal

We are currently investigating a potential cyber security incident.

· As a precaution, please do not use any systems identified as affected until further notice.

· Report anything unusual to **[insert contact details]** and please do not discuss the incident externally or on social media.

· Further updates will be provided as more information becomes available.

### External

We are currently investigating an issue affecting some of our services.  Our teams are working to establish the cause and understand any potential impact. We will provide further updates as soon as verified information becomes available.

## Recommendation

Assume that your primary communication systems may not be available during a significant cyber security incident. Ensure alternative communication methods are documented, tested regularly, and understood by those responsible for managing the incident.

Having a trusted, independent means of communication can significantly improve coordination and decision-making during the critical early stages of an incident.



# RECOVERY, STAND DOWN, AND LESSONS LEARNED

## RECOVERY

Once the immediate threat has been contained, attention should turn to the safe recovery of services and normal business operations. Recovery activities should be prioritised according to business need and risk. The following recovery priorities should be considered:

- Protect life, welfare and safety.
- Maintain critical business services.
- Restore safe communications.
- Protect and recover key data.
- Restore finance, payroll and customer-facing systems.
- Restore remaining systems in a controlled manner.
- Verify that appropriate security checks and recovery measures have been completed before reconnecting systems, with residual risks assessed and accepted.
- Monitor systems for any signs of further malicious activity.

Recovery should be coordinated by the Incident Lead in consultation with IT support, business leaders and any external specialists involved in the response.

## STAND DOWN AND INCIDENT CLOSE

The Cyber Incident Response Plan should only be stood down once:

- The incident has been investigated.
- Appropriate recovery actions have been completed.
- Critical business services have been restored.
- Any required reporting has been completed.
- Senior leadership are satisfied that risks have been reduced to an acceptable level.

Relevant stakeholders, partners, suppliers and external agencies should be informed when the incident is formally closed.

## LESSONS LEARNED AND CONTINUOUS IMPROVEMENT

Every cyber incident provides an opportunity to improve resilience. As soon as reasonably practicable following the closure of an incident, a review should be conducted to identify:

- What happened.
- What worked well.
- What challenges were encountered.
- What actions could have been taken sooner.
- Whether plans, procedures or training require improvement.
- Any lessons that should be shared across the organisation.

Where possible, a short "hot debrief" should take place immediately after the incident, followed by a more detailed review at a later date. Any recommendations should be recorded, assigned to an owner and monitored through to completion.

A template Lessons Learned Report is provided in Appendix H.



# Appendix A Contacts Directory

| Organisation | Notes | Contact Details |
|---|---|---|
| Information Security Officer | | |
| Data Protection Officer | | |
| Insurance Company | | |
| Insurance Cyber Company | | |
| Incident Response Company | | |
| Solicitor / Legal Adviser | | |
| IT Point of contact | Office hours:<br>Out of hours: | |
| MSP | | |
| IT Company | | |
| Cloud Provider | | |
| Website Provider | | |
| Microsoft 365 Administrator | | |
| Domain Registrar | | |
| Banks | | |
| PR / Crisis Comms | | |
| Accountant | | |
| Payroll Provider | | |
| Critical Suppliers | | |

# Appendix A Contacts Directory (Continued)

| Organisation | Notes | Contact Details |
|---|---|---|
| Report Fraud | Provides the central point of contact for the reporting of fraud & cyber crime. Will forward details of the cyber security incident to the National Fraud Intelligence Bureau who analyses and then notifies the National Crime Agency. Neither Action Fraud nor the National Fraud Intelligence Bureau is responsible for the investigation of offences but record all Live cyber-attacks. | 0300 1232040 |
| Information Commissioner's Office | Data Protection Officer to make contact if a personal data breach is likely to result in a risk to individuals' rights and freedoms. The 72-hour period generally runs from awareness of a notifiable breach. | 0303 1231113 |
| National Cyber Security Centre | The NCSC may provide specialist advice, guidance or signposting depending on the nature and severity of the incident. | https://report.ncsc.gov.uk/ |
| National Crime Agency | Investigate the most serious and complex attacks hitting the UK. Co-ordinate and support the entire UK policing response as well as providing specialist high-end technical support. Assess the cyber security incident via the NCCU and allocate the appropriate agency to investigate. | |
| Regional Cyber Crime Unit | When tasked by the NCA may provide: Support the investigation into the cyber security incident. Assist during a cyber specific incident by providing cyber tactical representatives and advisors. Provide specialist knowledge and assistance in and out of hours through a national on-call rota. | |
| Sector regulators? | E.g. Charities Commission, Dept. of Ed, FCA, CQC, SRA | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Appendix B

A Cyber Security Incident has been declared by IT, information security, senior leadership team, or the business owner

Duty Manager to ensure initial actions are completed

What has happened?
How many people / devices affected?
What is the exact description of what has occurred?

Make a record in initial action on APPENDIX C
Give advice to staff APPENDIX E

What type of attack?

Attack on your systems

Notify IT point of contact → Activate IT Cyber Security Incident Plan

Notify Senior Leadership Team → Assess incident using Appendix F

Notify Information Security Officer → Activate Information Security Plan

Notify Data Protection Officer → Assess Incident

Notify Media Relations → Support internal and external messaging

Attack on supply chain

Notify IT point of contact → Assess possible impact

Notify Information

Notify Data Protection Officer

Notify Media Relations → Support internal and external

Notify Senior Leadership Team

Consider notification to Report Fraud

Activate Cyber Incident Response Team

Any impact?

Brief Strategic Manager using **Appendix G** → Appoint lead to mitigate impact on business

Set recovery, strategy, investigation → Activate business continuity plans

Monitor and review regularly

# Appendix C Incident Log

**This maintains a log of initial actions which will assist the senior leadership team and other supporting resources when allocated.**

Brief circumstances:

What exactly happened?

How many affected?

What is the impact?

| Time / Date | Person Completing | Log Note |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Appendix D Strategic Decision Log

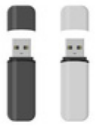
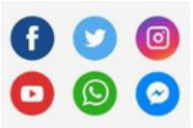
**During a cyber incident, decisions may need to be made quickly with incomplete information. This log should record key decisions, who made them, why they were made and what information was available at the time.** Examples of decisions to record:

- Decision to disconnect systems.
- Decision to invoke business continuity plans.
- Decision to notify customers, suppliers or regulators.
- Decision to report to ICO, police, insurer or other bodies.
- Decision to restore from backup.
- Decision to delay restoration to preserve evidence.
- Decision to issue internal or external communications.

| Time / Date | Decision Made | Decision Owner | Reason For Decision | Action Required |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Appendix E Advice to staff reporting cyber incident

## Action for first responders to follow if staff report a cyber incident

| | |
|---|---|
| Direct staff to IT support or the person responsible.<br>If out of hours, consider contacting the IT emergency contact. |  |
| Who else has been affected?<br>Is it just you or other people around you reporting the same or similar problems? |  |
| Do not turn off the computer, leave it turned on to ensure evidence is preserved. |  |
| Place sign on the computer to stop others using it. Provide the sign within this pack. |  |
| Isolate the computer by removing the network cable or put it in airplane mode if connected by Wi-Fi or bluetooth. |  |
| Secure any memory sticks, discs, DVDs, or any other media connected to or used in the computer. |  |
| Do not allow the user to take any remedial action or access their emails from another device. |  |
| Do not let the user log onto any other devices. |  |
| Do not post on social media or discuss the incident with anyone outside of your organisation. |  |
| Encourage the user to think about other ways they can continue their role and direct them to business continuity plans. |  |

# Appendix F Incident Lead / Manager Action Card

## Incident Lead / Tactical Manager / Senior Leadership Team / Duty Manager

| | |
|---|---|
| 1 | Coordinate the organisations response to a cyber incident. You will arrange and chair an internal meeting to achieve this. |
| 2 | What is the scale of the reported incident? Has it formally been declared a cyber incident by IT, Information Security, senior leadership team, or business owner? Any member of staff may report or escalate a suspected cyber incident. Formal declaration should be made by the most appropriate responsible person available. |
| 3 | Has contact been made with the person responsible for IT? Has IT support or your MSP been engaged and have appropriate technical response actions been started? Has contact been made with the Information Security Officer and the Data Protection Officer? |
| 4 | Consider notifying Report Fraud? If yes, what feedback or intelligence has been passed? |
| 5 | Brief the duty media officer to prepare communications to staff as well as partners and the media. |
| 6 | Have any partners been notified that share IT systems that could also be infected? |
| 7 | Appoint leads for areas of operational business that may be impacted. This may be one person or many depending on the scale refer to business continuity plans. |
| 8 | Arrange an internal Cyber Incident Response Team meeting as soon as possible. It should include representatives from IT, Information Security, Data Protection, Communications, and Business Impact staff. |
| 9 | Brief strategic lead / Chief Executives ensuring there is a clear strategy set which balances the recovery systems against investigation. |
| 10 | Has the organisation's cyber insurance provider been notified? Many policies require notification within specific timescales. This is one of the most commonly missed actions during exercises. |

# Appendix G Business Lead Action Card

## Business Lead / Strategic Manager / Senior Leadership Team / Chief Executives

| | |
|---|---|
| 1 | Appoint leads for areas of operational business that may be impacted. This may be one person or many depending on the scale refer to business continuity plans. |
| 2 | What is the current impact of this incident on the company? Is this a widespread national incident or restricted to you only? Are there any other partners also affected? |
| 3 | Balance the need to restore IT systems with the requirement to preserve evidence for investigation. Agree and document which activities take priority. |
| 4 | Has a Cyber Incident Response Team meeting been formed to manage this incident? This is the group that should be chaired by the senior leadership team to drive your response. |
| 5 | Has contact been made with Report Fraud / National Cyber Security Centre, where appropriate? If so, what was their assessment, advice, or support they have offered? |
| 6 | Your information management department should consider the reporting of any incident to the Information Commissioners Office which is time critical. They should also brief the Senior Information Owner. They may not be a 24/7 department so check their functions are being carried out within the time scales. |
| 7 | Does this incident have any impact on your supply chain? Is it likely that the cyber-attack will attract their oversight? |
| 8 | Establish a safe and accessible location or alternative communication arrangement for the response team. |
| 9 | Agree a lead, identify priorities, resource, and capabilities for an effective response, including times of further meetings. Communicate using plain English, try to avoid jargon. |
| 10 | Jointly understand the risk, share information about the likelihood and potential impact, to agree control measures and risk reduction. |

# Appendix H Lessons Learned Action Card

**Submission of this report will instigate a review of the plan by the senior leadership team which is vital for continuous improvement.**

- What happened? When did it start? How was it discovered?
- What worked well? Were communications effective?
- What caused delay or confusion?
- Were contact details correct? Were staff clear on what to do?
- Were backups available and usable? Were backups tested before the incident?
- Were third-party suppliers involved and did they respond effectively?
- What needs changing within 7 days, 30 days and 90 days?

| | |
|---|---|
| Name of Plan implemented | |
| Date and time implemented | |
| Person implementing | |
| Brief Circumstances | |
| What went well | |
| What could be improved within the plan to help you next time? | |

Appendix I



# Cyber Action

Discover or suspect a Cyber Incident?

Confirm infected devices are disconnected from network?
Consider disconnecting network from the internet.
Utilise a secure separate conference call to understand what has happened and review the impact

**Insert Conference Call Number**

**Insert Chair persons & participants dial in code**

Consider representatives from Insurance, Legal, PR, IT, HR & Law Enforcement?
Allocate someone to track incident/actions/maintain a written log
Preserve all device / server logs

Confirm containment steps?
Identify source and ensure other users are not exposed?
Consider password resets (users / administrators / systems)
Confirm availability of CLEAN back-ups?
Consider steps to eradicate and the recovery phase?
Have you secured evidence?
Keep an infected device, disconnected and available for police
Run anti-virus check / malware protection on all devices / Consider fresh install
Reconnect to network only when safe
Containment, investigation, and recovery actions should be coordinated by the appointed technical lead. Avoid making changes that could destroy evidence or increase disruption.

Consider reporting incidents to the Police through Report Fraud 0300 123 2040
Consider your disclosures?
Voluntarily - Internal / External / Press Releases
Personal data breach — assess whether ICO notification is required.
Regulatory - E.g. Dept of Ed. / Charities Commission / FCA / CQC
Review lessons learned

Appendix J



# Cyber Action

Discover or suspect a Cyber Incident?

## STOP AND CONTAIN

- Stop using the affected device immediately and disconnect from Wi-Fi or unplug its network cable, where safe.
- If several devices appear affected, consider disconnecting the internet connection to prevent further spread, but be aware this may interrupt essential services.
- Do not switch off, restart, wipe or rebuild affected devices unless necessary for safety or advised by a specialist.
- Place a DO NOT USE sign on affected devices.
- Keep connected USB drives and other removable media safe. Do not connect them to another device.

## ALERT THE RIGHT PEOPLE

**Contact Senior Leadership Team**

**Insert Name & number**

**Contact person responsible for IT**

**Insert Name & number**

## RECORD WHAT HAPPENED

- Note what you were doing when the problem appeared.
- Record the time, affected devices and any unusual messages.
- Photograph the screen if safe to do so.
- Preserve evidence and keep a record of actions taken.

Appendix K

# STOP

# DO NOT USE



**Person responsible for IT informed date:**
**Reference No:**


# STOP

# DO NOT USE





**Person responsible for IT informed date:**
**Reference No:**

# Appendix L Version Control

| Version | Comments/Changes | Editor | Date |
|---|---|---|---|
| **1.4** | Creation and initial edits | Chris White | 20/9/21 |
| **1.5** | Refresh content | Chris White | 5/4/23 |
| **1.6** | Edits | Chris White | 7/6/23 |
| **1.7** | Edits | Chris White | 15/7/24 |
| **1.8** | Refresh content | Chris White | 25/5/26 |
| **1.9** | Refresh content | Chris White | 17/10/26 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |