NUTFIELD CHURCH (C OF E) PRIMARY SCHOOL

Cyber Response Plan

Vision

We fully embrace the vision stated in the Church of England's Vision for Education 'Deeply Christian Serving the Common Good' published in July 2016 of educating the whole person. We aim for our children and members of the wider school community to flourish in all they do and **'live life in all its fullness'.** (John 10:10)

Values

- We are a church school, which believes in the importance of **community**, where people from all races, religions and cultures act in **peace** together.
- Our pupils, staff and families work together as a team, with **wisdom** supporting each other through our learning. We have **hope** in our challenges and in our successes.
- We recognise the **dignity** and ultimate worth of each person, created in the image of God, further shaped by the person, teaching and example of Jesus. We look to the future with **joy.**

Policy Reviewed: **March 2023**

Next Review: **March 2024**

Contents

Introduction

The Cyber Response Plan has be considered, as part of an overall continuity plan, to ensure it maintain a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

If the school fails to plan effectively then recovery can be severely impacted, causing additional loss of data, time, and ultimately, reputation.

Incidents may occur during the school day or out of hours. The Cyber Response Plan will be tested, with input from key stakeholders, to ensure that in an emergency there is a clear strategy, which has fail-safes when key personnel are unavailable.

The plan covers all essential and critical IT infrastructure, systems, and networks. The plan will also ensure that communications can be quickly established whilst activating cyber recovery.

This policy is based on a document produced by the Derbyshire County Council Education Data Hub. Additional cyber resilience resources for schools are available at Resources - Education Data Hub.

Aims of a Cyber Response Plan

The aim of the Cyber Response Plan, is to establish who will be involved in the Cyber Recovery Team, to ensure that in the event of a cyber-attack, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

In addition the plan will identify critical data assets and how long we would be able to function without each one, establish plans for internal and external communications and have thought about how we would access registers and staff and pupil contact details.

This will allow us to:

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

Risk Protection Arrangement (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."
Our RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident, the school must contact RPA Emergency Assistance by telephone: 0800 368 6378 or by email: RPAresponse@CyberClan.com.

To be eligible for RPA Cyber cover, there are 4 conditions that members must meet:

1. **Offline backups:** It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups. With our backups we the following:
    a) Back up the right data
    b) Backups are held fully offline and not connected to systems or in cold storage.
    c) Backups are tested appropriately, and run daily.

    JSPC Computer Services Ltd, our third-party IT support provider, facilitate our backups and they have given the following statement:

    "Your systems are protected by Altaro VM backups. There is a digital disconnect by dint of the fact that the backup software runs on your Host server, and as such your main servers have no direct access to this Host. The password for the Host is different to all your other passwords, and in order to access the backups you also need a separate encryption key, which is not stored on any of your systems."

2. **Undertake NCSC Cyber Security Training:** All employees or Governors who have access to the schools information technology system must undertake NCSC Cyber Security Training. It is available as a 36 minute video that can be distributed to all staff to watch individually when they have time. Completion can be recorded centrally by the School Business Manager and in the event of a claim the school will be required to provide this evidence.

3. **Register with Police CyberAlarm:** Registering will connect the school with their local police Cyber Protect team. The tool will record traffic on the network without risk to personal data.

4. **Have a Cyber Response Plan in place.**

Preparation and Additional Measures

It is vital that we regularly review our existing defences and take the necessary steps to protect the school network. In addition to the 4 conditions of cover detailed above, there are other measures which we have implement to help improve our IT security and mitigate the risk of a cyber-attack:

- All staff read and sign the schools Acceptable Use document which covers the use of IT equipment and school devices.
- Regularly review the Emergency Plan, Cyber Response Plan and Data Protection Policy.
- Monitor and review firewall rules.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.
- Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit.
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

Actions in the event of an incident

If you suspect you have been the victim of a ransomware or other cyber incident, you should take the following steps immediately:

1. Inform the School Business Manager or Headteacher who will

2. Enact the Cyber Recovery Plan

3. Contact the 24/7/365 RPA Cyber Emergency Assistance:
   - By telephone: 0800 368 6378 or by email: RPAresponse@CyberClan.com
   - You 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.

4. Inform the National Cyber Security Centre (NCSC) - https://report.ncsc.gov.uk

5. Contact your local police via the Action Fraud website or call 0300 123 2040

6. If you are a part of a Local Authority (LA), they should be contacted

7. Contact your Data Protection Officer (the School Business Manager)

8. Consider whether reporting to the ICO is necessary report at www.ico.org.uk or by calling 0303 123 1112

9. Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

Please be aware that 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.

Cyber Recovery Plan

1. Verify the initial incident report as genuine and record on the Incident Recovery Event Recording Form at Appendix C.

2. 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.

3. In the event of a suspected cyber-attack contact JSPC, IT support, to isolate devices from the network.

4. In order to assist data recovery, if damage to a computer or back up material is suspected, staff should not:
   - Turn off electrical power to any computer.
   - Try to run any hard drive, back up disc or tape to try to retrieve data.
   - Tamper with or move damaged computers, discs or tapes.

5. Contact RPA Emergency Assistance Helpline. By telephone: 0800 368 6378 or by email: RPAresponse@CyberClan.com

6. Start the Actions Log to record recovery steps and monitor progress.

7. Convene the Cyber Recovery Team (CRT).

8. Liaise with JSPC, IT support, to estimate the recovery time and likely impact.

9. Make a decision as to the safety of the school remaining open.
   - This will be in liaison with relevant Local Authority Support Services.

10. 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 school's Data Protection Officer and the police

11. Execute the communication strategy which should include a media / press release if applicable.
    - Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.

12. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.

13. Upon completion of the process, evaluate the effectiveness of the response using the Post Incident Evaluation at Appendix D and review the Cyber Recovery Plan accordingly.

14. Educate employees on avoiding similar incidents / implement lessons learned.

Cyber Recovery Team (CRT)

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 School	Contact Details
Recovery Team Leader	Imogen Woods	Headteacher	head@nutfield.surrey.sch.uk
Data Management	Daniel Walker-Cheetham	School Business Manager	bursar@nutfield.surrey.sch.uk
IT Restore / Recover	Daniel Walker-Cheetham	School Business Manager	bursar@nutfield.surrey.sch.uk
Site Security	Fred Kolndreu	Premises Manager	Fred.Kolndreu@nutfield.surrey.sch.uk
Public Relations	Imogen Woods	Headteacher	head@nutfield.surrey.sch.uk
Communications	Serena Fowler	School Office Manager	info@nutfield.surrey.sch.uk
Resources / Supplies	Serena Fowler	School Office Manager	info@nutfield.surrey.sch.uk
Facilities Management	Fred Kolndreu	Premises Manager	Fred.Kolndreu@nutfield.surrey.sch.uk

Server Access

Below is a list of people with administrative access to the server:

Role	Name	Contact Details
Third Party IT Provider	JSPC Computer Services Ltd	01903 767122

Management Information System (MIS) Admin Access

Below is a list of people with administrative access to the MIS:

MIS Admin Access	Name	Contact Details
School Business Manager	Daniel Walker-Cheetham	bursar@nutfield.surrey.sch.uk
MIS Support Provider	Strictly Education 4S	sims@strictlyeducation.co.uk

The procedures and details above should not be published with contact details included due to the risk of a data breach.

Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server	On-site (HDD) and off-site (Cloud)	Daily
School MIS	On-site (HDD) and off-site (Cloud)	Daily
Email Server	Off-site (Cloud)	Daily
Curriculum Files	On-site (HDD) and off-site (Cloud)	Daily
Teaching Staff Devices	On-site (HDD) and off-site (Cloud)	Daily
Administration Files	On-site (HDD) and off-site (Cloud)	Daily
Finance / Purchasing	On-site (HDD) and off-site (Cloud)	Daily
HR / Personnel Records	Paper records, some information is on the server and backed up on-site (HDD) and off-site (Cloud)	Daily
Inventory	Paper records, some information is on the server and backed up on-site (HDD) and off-site (Cloud)	Daily
Facilities Management	Paper records, some information is on the server and backed up on-site (HDD) and off-site (Cloud)	Daily

Key Contacts

	Supplier	Telephone Number	Account / Reference Number
Internet Connection	Talk Straight – Schools Broadband	01133 222 333	Nutfield Church Primary School – RH1 4JJ
Backup Provider	JSPC Computer Services Ltd	01903 767 122	Nutfield Church Primary School
Telecom Provider	Excell Network Solutions Ltd	08001 959 959	013779
Website Host	Frootes Media	07701 021 649	NUT001
Electricity Supplier	EDF Energy	105	7177184487
Burglar Alarm	Admiral Security	01737 855 900	NUTFIE
Keyholders	Knight Security	01276 469 988	Nutfield Church Primary School – RH1 4JJ
Parent/Carer Contact System	IRIS ParentMail	03448 155 555	CU0011876
Action Fraud	-	03001 232 040	N/A
Legal Representative	Surrey County Council	020 8541 9128	Nutfield Church Primary School

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: Miss Imogen Woods Role: Headteacher

Name: Mrs Serena Fowler Role: School Office Manager

Key Roles and Responsibilities

Headteacher (with support from Deputy Head / School Business Manager)

- 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 Governors.
- Liaises with the school 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 / pupils.
- Liaises with School Office Manager to contact parents, if required, as necessary

Designated Safeguarding Lead (DSL)

- Seeks clarification as to whether there is a safeguarding aspect to the incident.
- Considers whether a referral to Cyber Protect Officers / Early Help / Social Services is required.

Premises Manager

- Ensures site access for external IT staff at JSPC.
- Liaises with the Headteacher to ensure access is limited to essential personnel.

School Business Manager (SBM)

- 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 school is.
- Contacts relevant external agencies – RPA Emergency Assistance / IT services / technical support staff

Data Protection Officer (DPO)

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

School Office Manager

- Manages the communications, website / texts to parents / school emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

Chair of Governors

- Supports the Headteacher 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 governors 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 school policy.

JSPC IT Support

- Verifies the most recent and successful backup.
- Liaises with the RPA Incident Response Service to assess whether the backup can be restored or if server(s) themselves are damaged, restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss.
- Liaises with the Headteacher and School Business Manager as to the likely cost of repair / restore / required hardware purchase.
- Provides an estimate of any downtime and advises which systems are affected / unaffected.
- If necessary, arranges for access to the off-site backup.
- Protects any records which have not been affected.
- Ensures on-going access to unaffected records.

Teaching Staff and Teaching Assistants

- Reassures pupils, staying within agreed pupil standard response
- Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed

Critical Activities – Data Assets

Below is a list data assets the school has access to which have been categorised by criticalness and how long we would be able to function without each one.

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Leadership and Management	Access to Headteacher's email address	4 hours	No
	Access to School Business Managers email address	4 hours	No
	Access to School Office (info@) email address	4 hours	No
	Head's reports to governors (past and present)	1 week	No
	Key stage, departmental and class information	4 hours	No
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns	4 hours	No
	Attendance registers	4 hours	No
	Referral information / outside agency / TAFs	12 hours	No
	Child protection records	12 hours	No
	Looked After Children (LAC) records / PEPs	12 hours	No
	Pupil Premium pupils and funding allocations	12 hours	No
	Pastoral records and welfare information	4 hours	No
Medical	Access to medical conditions information	48 hours	Yes
	First Aid / Accident Logs	12 hours	Yes
Teaching	Schemes of work, lesson plans and objectives	12 hours	No
	Teaching resources, such as worksheets	12 hours	Yes
	Learning platform / online homework platform	12 hours	Yes
	Curriculum learning apps and online resources	12 hours	Yes
	CPD / staff training records	1 week	No
	Pupil reports and parental communications	4 hours	No
SEND Data	SEND List and records of provision	12 hours	No
	IEPs / EHCPs / GRIPS	12 hours	No
Conduct and Behaviour	Reward system records, including house points or conduct points	72 hours	Yes
	Behaviour system records, including negative behaviour points	72 hours	Yes
	Sanctions	72 hours	Yes
	Exclusion records, past and current	72 hours	Yes
	Behavioural observations / staff notes and incident records	72 hours	Yes
Assessment and Exams	Exam entries and controlled assessments	4 hours	No
	Targets, assessment and tracking data	72 hours	No
	Baseline and prior attainment records	72 hours	No
	Exam results	24 hours	No
Governance	School development plans	72 hours	No
	Policies and procedures	24 hours	No
	Governors meeting dates / calendar	24 hours	No
	Governor attendance and training records	1 week	No
	Governors minutes and agendas	1 week	No

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Administration	Admissions information	12 hours	No
	School to school transfers	12 hours	No
	Transition information	12 hours	No
	Contact details of pupils and parents	4 hours	Yes
	Access to absence reporting systems	4 hours	No
	School diary of appointments / meetings	4 hours	No
	Letters to parents / newsletters	4 hours	No
	Extra-curricular activity timetable and contacts for providers	4 hours	No
	Census records and statutory return data	72 hours	No
Human Resources	Payroll systems	4 hours	No
	Staff attendance, absences, and reporting facilities	4 hours	No
	Disciplinary / grievance records	4 hours	No
	Staff timetables and any cover arrangements	4 hours	No
	Contact details of staff	4 hours	No
Office Management	Photocopying / printing provision	12 hours	No
	Telecoms - school phones and access to answerphone messages	4 hours	No
	Email - access to school email systems	4 hours	No
	School website and any website chat functions / contact forms	24 hours	No
	Management Information System (MIS)	4 hours	No
	School payments system (for parents)	12 hours	No
	Financial Management System - access for orders / purchases	12 hours	No
Site Management	Site maps	1 week	Yes
	Maintenance logs, including legionella and fire records	48 hours	Yes
	Risk assessments and risk management systems	48 hours	No
	COSHH register and asbestos register	48 hours	Yes
Catering	Payment records for food & drink	24 hours	No
	Special dietary requirements / allergies	4 hours	Yes

Appendix A: Incident Impact Assessment

Use these tables 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 school'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 school 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 school can no longer provide any critical services to users. It is likely the school 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 school 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 school.
	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.

Appendix B: Communication Templates

School Open

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down [some / all] of the school 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 school 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 / GDPR. Every action has been taken to minimise disruption and data loss.

The school 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 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 pupils and staff. The school 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 school 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,

School Closure

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down the school 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 school 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 / 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 pupils and staff.

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

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 school 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,

Staff Statement Open

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

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

(Detail any workarounds / changes)

The school 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 / 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 school 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]

Staff Statement Closed

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

(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will close to pupils [on DATE or with immediate effect].

(Detail staff expectations and any workarounds / changes or remote learning provision)

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

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school 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].

Media Statement

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

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

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

A standard staff response for serious IT incidents should reflect only information which is already freely available and has been provided by the school 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 / school website / other pre-determined communication route.

Standard Response for Pupils

For staff responding to pupil requests for information, responses should reassure concerned pupils 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 pupils that this has been confirmed in letters / emails to parents / carers.

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

Appendix C: 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.

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

Relevant Referrals

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

Actions Log

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

Appendix D: 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:		