Department for Education

The Federation of the Church Schools of Shalfleet and Freshwater & Yarmouth

Together for a Brighter Future

Risk Protection Arrangement

Cyber Security & Response Plan

The Federation of the Church Schools of

Freshwater & Yarmouth and Shalfleet

Last Reviewed	Spring 2026
Reviewed By	MD – Governor
Next Review Date	Spring 2027

Contents

1. Introduction. 3

2. Aims of a Cyber Response Plan 3

3. Current Back Up Systems in Place 4

4. Preparation and Additional Resources 7

5. Actions in the event of an incident 8

6. Cyber Recovery Plan 9

Appendix A: Incident Impact Assessment 17

Appendix B: Communication Templates 19

Appendix C: Incident Recovery Event Recording Form 24

Appendix D: Post Incident Evaluation. 2

1. Introduction

A Cyber Response Plan is part of an overall continuity plan to ensure that a minimum level of functionality is maintained to safeguarding pupils and staff and to restore the school back to an operational standard.

If a 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 should 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 ensure that communications can be quickly established whilst activating cyber recovery. The plan will be well communicated and readily available.

This document is 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.

2. Aims of a Cyber Response Plan

The Cyber Response Plan considers who will be involved in the Cyber Recovery Team, key roles and responsibilities of staff, what data assets are critical and how long the school would be able to function without each one, establish plans for internal and external communications and how the school would access registers, staff and pupil contact details. This is to ensure:

- Immediate and appropriate action is taken in the event of an IT incident.
- Prompt internal reporting and recording of incidents
- Immediate access to all relevant contact details (including backup services and IT technical support 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.

3. Current Back Up Systems in Place

Preparation and Additional Resources

As a school it is vital that we regularly review our existing defences and take the necessary steps to protect the networks. There are several measures that the school can implement to help improve IT security and mitigate the risk of cyber-attack.

- Regularly review Data Protection Policy
- Access current security measure against Cyber Essential requirements, such as firewall rules, malware protection, and role-based user access.

- Ensure Multi-Factor Authentication (MFA) is in place
- Implement a regular patching regime. Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit.
- Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible.
- Review NCSC advice regarding measures for IT teams to implement.
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

School Response – The Current Procedure for the Back-Up of Data

On Site – USB Disks

The School currently uses 3 USB attached hard drives to perform nightly backups. These disks are not encrypted and do not leave site. The disks are rotated in such a way as to provide a weekly or daily recovery option. 1 disk is only ever attached to the Server limiting exposure to malware and ransomware. The backup regime is documented and the changing of the disk is the responsibility of the school's administrator. Email notifications are sent out on completion of the backup as a reminder to change the disk.

Recovery is only necessary where an entire virtual machine has failed. Individual file recovery is possible albeit lengthy using a scratch disk as an intermediate medium.

On Site – NAS (Network Attached Storage)

The School has a 2 disk NAS used for archiving and backup. The NAS has 2FA (2 factor authentication) enabled. Nightly SIMS/FMS databases are copied to the NAS. Weekly staff/student data is copied to the NAS. Weekly virtual machines data is copied to the NAS (2 iterations). Archive data is copied to the NAS as and when required. The NAS is mounted only at the time of backup and disconnected at all other times. The NAS is only accessible from within the school network.

Recovery is done via mounting the NAS and copying the data required.

On Site – VSS (Volume Shadow Copy)

The main file server uses VSS to create 3 copies of data at 09:00, 12:00 & 17:00 daily for 30 days. This allows immediate data recovery at a user level.

Recovery is performed by the user by selecting "restore previous version" from within file explorer and selecting a time/data and copying the lost data back.

Off Site – USB Disk

Wight Support hold an encrypted backup offsite in a Fire/Water safe. This is created at the end of each complete term and restored to an offsite encrypted server to test recoverability. This back up is a last resort and is tested each term for completeness.

Recovery is only necessary where an entire virtual machine has failed. Individual file recovery is possible albeit lengthy using a scratch disk as an intermediate medium.

Off Site – Google Drive

The NAS mirrors the SIMS/FMS databases, staff/student data and archive data. The Google drive is secured by a randomly generated complex password. Data is encrypted using 256bit AES client-side encryption on the NAS with a randomly generated complex password and synchronised out of hours.

Recovery is performed by assessing the Google drive and copying the data back. The data is not readable natively and only accessible using a proprietary piece of software provided by the NAS manufacturer and having access to the AES client-side encryption key.

Current Provision in Place

Antivirus

The school uses Avast for Business as its Virus protection. This is a business antivirus product that offers real time file scanning, email scanning, web shield and data shredder. Email alerts are set up to notify us of the virus intrusion or failure to report in.

Firewall

Standard Windows firewalls are enabled on both client computers and servers with rules to allow domain traffic. School also uses a Draytek Router which limits/blocks ports from access.

VPN

The school allows remote connection using RRAS (Routing and Remote Access Service) and NPS (Network Policy Server). Connections use L2TP as the protocol with a shared key between the client computer and the server. The user must also be a member of the allowed VPN access group. We do not monitor log files for intrusion as external access is limited by user, group membership and security key.

Administrative Access

Staff do not have administrative access to be able to run/install products on their machines unless explicitly requested. This limits exposure to being able to run unwanted files.

Current Filtering Provisions

Web Filtering

The school currently uses web filtering provided by Lightspeed Systems. The filtering is DfE approved and offers split filtering based on user groups. Currently the school has one group for staff based on email address that allows website exceptions. All other users are subject to the default rules as are BYOD (Bring Your Own Device). Staff computers have a Lightspeed Client installed that reports all sites visited by each individual member of staff. There is also a global overview for the site which shows top sites visited, top searches and blocked sites.

1. All Employees who have access to the Member's information technology system (MIS) must undertake NCSC Cyber Security Training by 31st May 2022. 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.

   This action has been implemented.

2. Register with Police Cyber Alarm. 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.

3. Have a Cyber Response Plan in place.

With current procedures in place, in the event of a cyber-attack the following timeline would apply:

Within 24 hours - the infrastructure would be restored
Within 48 hours - administrative processes would be restored
Within 72 hours – teaching systems would be restored
Within 1 week – pupil information would be restored

Acceptable Use

The school will ensure that all users will receive and read all of the relevant policies and acceptable use/loan agreements for school devices.

Please be aware if an incident is found to be caused by misuse, this could give rise to disciplinary measures and referral to the police.

Communicating the Plan

The Cyber Recovery Plan will be communicated to all those who are likely to be affected and will ensure that key staff are informed of their roles and responsibilities in the event of an incident, prior to any issues arising.

Testing and Review

During an incident there can be many actions to complete, and each step should be well thought out, cohesive, and ordered logically.

Key staff members will be trained so that they feel confident following and implementing the plan. The plan will be reviewed regularly to ensure contact details are up-to-date and new systems have been included.

Templates are available, please see appendix's

4. Actions in the event of an incident

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

- Contact a member of SLT
- Enact the Cyber Recovery Plan
- 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.

- Inform the National Cyber Security Centre (NCSC) – https://report.ncsc.gov.uk
- Contact the local police via Action Fraud, Action Fraud website or call 0300 123 2040
- Contact the Local Authority
- Contact the Data Protection Officer
- Consider whether reporting to the ICO is necessary, take guidance from DPO. ICO number 0303 123 1112
- Contact the Sector Security Enquiries Team at the Department for Education by emailing: sector.securityenquiries@education.gov.uk

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.

5. 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, IT staff should 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.
6. Start the Actions Log to record recovery steps and monitor progress.
7. Convene the Cyber Recovery Team (CRT)
8. Liaise with IT staff 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. Adjust 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.

Ensure that this plan is kept up-to-date with new suppliers, new contact details, and changes to policy.

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:

Recovery Team Leader	Name	Role in School	Contact Details
Data Management	Sarah Woodburn Mark Flanders	School Business Manager Wight Support	01983760345 07581080076
IT Restore/Recover	Mark Flanders	Wight Support	07581080076
Site Security Public	Sarah Woodburn	School Business Manager	07729204546
Relations	Elizabeth Grainger	Headteacher	07825209605
Communications	Elizabeth Grainger Sarah Woodburn	Headteacher School Business Manager	07825209605 07729204546
Resources/Supplies	Sarah Woodburn Victoria Plumley	School Business Manager Finance Manager	07729204546 07971623014
Facilities Management	Sarah Woodburn	School Business Manager	07729204546

Server Access

Role	Name	Contact Details
Third Party IT Provider	Mark Flanders – Wight Support	07518080076

Management Information System (MIS) Admin Access

MIS Admin Access	Name	Contact Details
School Business Manager	Sarah Woodburn	07729204546
Wight Support	Mark Flanders	07581080076
MIS Provider	ESS Capita	0333 0150 212
Data Manager	Stuart Cook	07875009877

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

- Register
- Staff/Pupil contact details
- Current Child Protection Concerns

Backup Strategy

The current procedure for the back-up of data

Detail the process, frequency, procedure of reinstallation of data, confirm testing of the back-up process

On Site - USB Disks
- The School currently uses 3 USB attached hard drives to perform nightly backups. These disks are not encrypted and do not leave site. The disks are rotated in such a way as to provide a weekly or daily recovery option. 1 disk always remains in the school's fire safe. 1 disk is only ever attached to the Server limiting exposure to malware and ransomware. The backup regime is documented and the changing of the disk is the responsibility of the school's administrator. Email notifications are sent out on completion of the backup as a reminder to change the disk.
- Recovery is only necessary where an entire virtual machine has failed. Individual file recovery is possible albeit lengthy using a scratch disk as an intermediate medium.

On Site - NAS (Network Attached Storage)
- The School has a 2 disk NAS used for archiving and backup. The NAS has 2FA (2 factor authentication) enabled. Nightly SIMS / FMS databases are copied to the NAS. Weekly Staff / Student Data is copied to the NAS. Weekly Virtual Machines data is copied to the NAS (2 iterations). Archive data is copied to the NAS as and when required. The NAS is mounted only at the time of backup and disconnected at all other times. The NAS is only accessible from within the school network.
- Recovery is done via mounting the NAS and copying the data required.

On Site – VSS (Volume Shadow Copy)
- The main file server uses VSS to create 3 copies of data at 09:00, 12:00 & 17:00 daily for 30 days. This allows immediate data recovery at a user level.
- Recovery is performed by the user by selecting "restore previous version" from within file explorer and selecting a time / data and copying the lost data back.

Off Site – USB Disk
- Wightsupport hold an encrypted backup offsite in a Fire / Water safe. This is created at the end of each complete term and restored to an offsite encrypted Server to test recoverability.
- This is a backup of last resort and is tested each term for completeness. Recovery is only necessary where an entire virtual machine has failed. Individual file recovery is possible albeit lengthy using a scratch disk as an intermediate medium.

Off Site – Google Drive
- The NAS mirrors the SIMS / FMS Databases, Staff / Student Data and archive data. The Google drive is secured by a randomly generated complex password. Data is encrypted using 256bit AES client-side encryption on the NAS with a randomly generated complex password and synchronised out of hours.
- Recovery is performed by accessing the Google drive and copying the data back. The data is not readable natively and only accessible using a proprietary piece of software provided by the NAS manufacturer and having access to the AES client-side encryption key.

The current level of cyber protection/firewalls against cyber attacks

Current provision in place

Antivirus
The school uses Avast for Business as its Virus protection. This is a business antivirus product that offers real time file scanning, email scanning, web shield and data shredder. Email alerts are setup to notify us of Virus intrusion or failure to report in.

Firewall
Standard Windows firewalls are enabled on both client computers and Servers with rules to allow domain traffic. The school also uses a Draytek Router which limits / blocks ports from access.

VPN
The school allows remote connection using RRAS (Routing and Remote Access Service) and NPS (Network Policy Server). Connections use L2TP as the protocol with a shared key between the client computer and the Server. The user must also be a member of the allowed VPN access group. We do not monitor log files for intrusion as external access is limited by user, group membership and security key.

Administrative Access
Staff do not have administrative access to be able to run / install products on their machines unless explicitly requested. This limits exposure to being able to run unwanted files.

The current filtering provisions

Detail the current provision in place, the level of filtering and restrictions

Web Filtering
The school currently uses web filtering provided by Lightspeed Systems. The filtering is DfE approved and offers split filtering based on user groups. Currently the school has one group for staff based on email address that allows web site exceptions. All other users are subject to the default rules as are BYOD (Bring Your Own Device). Staff computers have a Lightspeed Client installed that reports all sites visited by each individual member of staff. There is also a global overview for the site which shows tops sites visited, top searches and blocked sites.

Business Continuity, should a cyber-attack occur

Short, medium and long-term plan following a cyber-attack

The school has multiple divorced backups from both the previous day, weekend and the end of the last term.

Server
Assuming the main host server can be accessed this can be wiped and restored in 24 hours. Often, where there has been a Cyber-attack, the Police may remove the Server for investigation. It should be considered lost at that point as this can be up to an 18-month delay before it's returned. A spare host which is available to schools as a short-term measure and is sufficient to run most environments.

Clients
Assuming a crypto virus attack, all clients would need to be wiped and reloaded. This is a time-consuming task and priority should be given admin staff followed by Teaching staff and then students. As soon as the server becomes available, admin staff 24 hours, Teaching staff a further 24 hours and students 48 hours. Realistically, from the point of attack, 2 days to have an admin function, 3 days for Teaching and 5 days students.

Prevention and mitigation against a cyber attack

The school utilises standard inbuilt Windows firewalls. These offer little to no reporting. Monitoring Windows logs is a post event time consuming process. The school also use a Draytek Router which does have basic DoS and Spoofing protection with post event logging.

As the school uses Google as it's email provider, they automatically scan emails for viruses and should annotate the email as having a virus if one is found. However, commercial email scanning products exist where an email is routed to them first for enhanced scanning.

Key Contacts

Supplier	Contact/Tel Number	Account/Reference Number
Internet Connection	E2BN – Shalfleet - 01462 833300 Wight Support - Yarmouth	
Backup Provider	Wight Support Light Speed	
Telecom Provider Yarmouth	Intech – 02380 242525 support@intechgroup.co.uk	ITT05975
Telecom Provider Shalfleet	BT 0800 800 154	SD44830373
Website Host	Foundation Media 01983 550415	N/A
Electricity Supplier	Zenergie – Chris Hazelden 023 8028 6304 SSE (Shalfleet) SEFE (Yarmouth)	
Intruder Alarm (Yarmouth)	Wessex Fire & Security – 01747 852258	669434028
Action Fraud	0300 123 2040	N/A
Local Constabulary	101	
Legal Representative	IWCC – 01983 821000	N/A
Police Cyber Alarm	Installed – running in the background	
LA/Trust Press Officer	IWCC – 01983 823739 Out of hours – 01983 821105	N/A

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: Elizabeth Grainger Role: Headteacher

Name: Sarah Woodburn Role: School Business Manager

Key Roles and Responsibilities

Headteacher (with support from Deputy Head/School Lead/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 Business 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.

Site Manager/School Business Manager

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

School 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 school is.
- Contacts relevant external agencies – RPA Emergency Assistance/IT services/technical support staff.
- Manages the communications, website/texts to parents/school emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

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.

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.

IT Lead/IT Staff

- 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 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

The list below details the school access, which are critical and how long the school 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.

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

Critical Activities	Data item required for service continuity	When required	Workaround? (Yes/No)	Paper Based Y/N
Leadership and Management	Access to Headteacher's email address	4 hours	Yes	N
	Minutes of SLT meetings and agendas	1 month	Yes	N
	Head's reports to governors (past and present)	1 month	Yes	N
	Key stage departmental and class information	12 hours	No	N
Safeguarding/ Welfare	Access to systems which report and record safeguarding concerns	12 hours	No	N
	Attendance registers	1 week	Yes	N
	Class group/teaching groups/staff timetables	1 week	Yes	N
	Referral information/outside agency/TAFs/Child protection records	12 hours	No	N
	Looked After Children (LAC) records/PEPs	12 hours	No	N
	Pupil Premium pupils and funding allocations	1 month	Yes	N
	Pastoral records and welfare information	1 week	No	N
	Access to medical conditions information	N/A	Yes	Y

Medical	Administration of medicine	N/A	Yes	Y
	First Aid/Accident Logs	N/A	Yes	Y
Teaching	Schemes of work, lesson plans and objectives	1 month	Yes	N
	Seating plans	N/A	N/A	N/A
	Teaching resources, worksheets	N/A	N/A	Y
	Learning platform/online homework platform/curriculum learning apps and online resources	12 hours	No	N
	CPD/staff training records	1 month	Yes	Y
	Pupil reports and parental communications	12 hours	No	N
SEND Data	SEND List and records of provision Accessibility tools	24 hours	No	N
	Access arrangements and adjustments	1 month	Yes	N
	IEPs/EHCPs/GRIPS	2 weeks	Yes	Y
Conduct and Behaviour	Reward system records, including house points or conduct points	1 month	Yes	Y
	Sanctions	1 month	Yes	Y
	Behavioural observations/staff notes and incident records	1 month	Y	N
	Exclusions records, past and current	1 month	Y	N
Assessment and Exams	Exam entries and controlled assessments	1 week	Y	N
	Targets, assessment and tracking data	1 month	N	N
	Baseline and prior attainment records	1 month	N	N
	Exam timetables and cover provision	N/A	N/A	N/A

Governance	Exam results	2 months	No	N
	School development plans	2 months	Yes	N
	Policies and procedures	1 month	Yes	N
	Governors meeting dates/calendar	1 month	Yes	N
	Governor attendance and training records	1 month	Yes	N
	Governor minutes and agendas	1 month	Yes	Y
Administration	Admissions information	1 month	Yes	N
	School to school transfers	1 week	No	N
	Letters to parents/newsletters	1 week	Yes	N
	Extracurricular activity timetable and contacts for providers	1 month	Yes	Y
	Census records and statutory return data	1 month	Yes	N
	Contact details for staff	1 month	Yes	N
Human resources	Payroll systems	2 weeks	Yes	N
	Staff attendance, absences and reporting facilities	3 weeks	Yes	N
	Disciplinary/grievance records	1 month	Yes	N
	Contact details of staff	1 month	Yes	N
Office Management	Photocopying /printing provision	12 hours	Yes	N
	Telecoms – school phones and access to answerphone messages	4 hours	Yes	N
	Email – access to school email systems	12 hours	Yes	N
	School website	1 week	Yes	N

	Management Information System	12 hours	Yes	N
	School payments system (for parents)	12 hours	Yes	N
	Financial Management System – access for orders/purchases	24 hours	No	N
Site Management	Visitor sign in/out	1 week	Yes	Revert to paper
	CCTV access	24 hours	No	N
	Site Maps	N/A	Yes	Y
	Maintenance logs, including legionella and fire records.	Third party app used	Yes	Y (currently paper copies kept)
	Risk Assessments and risk management systems	Third party app used as well as paper copies	Yes	Y
	COSHH register and asbestos register	2 weeks	Yes	Paper and electronic copies kept
Catering	Third party supplier			

Appendix A: Incident Impact Assessment

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

1. School Open

Dear Parent/Carer,

I am writing to inform you that it appears that 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 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 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,

2. 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 outrage]. 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 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 [XXXXXXXXXXX].

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 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/dojo].

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 Local Authority 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 2019/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 Local Authority 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 the 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**

[Insert school name] detected a cyber-attack on [date] which has affected the school IT systems. Following liaison with the Local Authority 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)	Contracted By	Response

Actions Log

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

Appendix D: Post Incident

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		