Cyber Security Policy and Response Plan

Last Reviewed Date:	new	**Review Date:**	03/10/2025

School Business Manager:		**Date:**	14/10/2025
Headteacher:		**Date:**	13/11/2025

Date of Next Review:	November 2026

C O N T E N T S

1. Scope

This policy applies to:

- All staff, governors, volunteers, and contractors
- Any third parties with access to school data or IT systems

The DfE ask the school in the event of a cyber incident, it may be helpful to consider how you would access the following:

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

This Policy and Recovery Response Plan is part of an overall plan to ensure there is a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

2. Cyber Recovery Team

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

	Name	Role in School	Contact Details
Recovery Team Leader	Neil Ward	Headteacher	
Data Management	Beebug	IT Support	
IT Restore / Recover	Beebug	IT Support	
Site Security	Matt Cummings	Premises Manager	
Public Relations	Ellen-May Shipp	SLT	
Communications	Janet Warrington	SBM	
Resources / Supplies	Gill Bebee	Bursar/Admin	
Facilities Management	Matt Cummings	Premises Manager	

3. Server Access

People with administrative access to the server:

	Name	Role in School	Contact Details
Beebug	Clark MacDonald	IT Support	
Beebug	Jimmy Varnavide	IT Support	
Beebug	Stuart Vowles	IT Support	

4. Management Information System (MIS) Admin Access

People with administrative access to the MIS:

	Name	Role in School	Contact Details
SLT	Jane Connolly	Deputy Headteacher	
SLT	Ellen-May Shipp	Senior Leader	
Admin	Suzie Horton	Office Manager / HR	
Admin	Mason Emoli	HR Manager	
Admin	Gill Bebee	Bursar	
Admin	Janet Warrington	SBM	
All Class Teachers			

5. Backup Strategy

School Process	Backup Type (including on-site / off-site)	Frequency
Main File Server	On-site and off-site	Daily
School MIS Arbor	Off-site	Daily
Cloud Services	Off-site	Daily
Third Party Applications / Software	Off-site	Application dependant
Email Server	N/A	N/A
Curriculum Files	On-site and off-site	Daily
Administrative Files	On-site and off-site	Daily
Finance / Purchasing	On-site and off-site	Daily
HR / Personnel Records	On-site and off-site	Daily
Inventory	On-site and off-site	Daily
Website	Off-site	Daily
USBs / portable drives	Not in use	

6. Key Contacts

Supplier	Supplier	Contact Details	Account/ Ref no
Internet Connection	IHG Connectivity		
Backup Provider	Beebug		
Telecom Provider	Grapevine		
Website Host	Jolt Media		
Electricity Supplier	NPower		
Burglar Alarm	SECOM		
Text Messaging System	Arbor		
Local Constabulary	East Herts Police		
Legal Representative			
LA Press Officer			

7. Social 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.

Name: Neil Ward — Role: Head Teacher
Name: Jane Connolly — Role: Deputy Headteacher
Name: Ellen-May Shipp — Role: Senior Leader

8. Key Roles and Responsibilities

Headteacher

- ☐ 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 (CoG)
- ☐ Liaises with the school Data Protection Officer (DPO)
- ☐ 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 the School Business Manager (SBM) 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 Protection Officers / Early Help / Social Services is required.

Premises Manager

- ☐ Ensures site access for external IT staff.
- ☐ 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 the 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 (CoG)

- ☐ 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.
- ☐ Ensure 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 Support (Beebug)

- ☐ 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 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

- ☐ Ensures any temporary procedures for data storage / IT access are followed.

9. Critical Activities – Data Assets

What is critical, how long you would be able to function without each one i.e. timescale you believe is necessary for recovery.
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)
Leadership & Management	Access to the Headteacher's email address	4 hours	No
	Minutes of SLT meetings and agendas	24 hours	No
	Head's reports to governors (past and present)	24 hours	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	Yes - paperbased
	Class groups, and staff timetables Referral information / outside agency / TAFs	4 hours	No
	Child protection records Looked After Children (LAC) records / PEPs	4 hours	No
	Pupil Premium pupils and funding allocations	4 hours	No
	Pastoral records and welfare information	4 hours	No
Medical	Access to medical conditions information	4 hours	No
	Administration of Medicines Record	4 hours	No
	First Aid / Accident Logs	4 hours	No
Teaching	Schemes of work, lesson plans and objectives Seating plans	4 hours	No
	Teaching resources Learning Platforms	4 hours	No
	Curriculum learning apps and online resources	4 hours	No
	CPD / staff training records Pupil reports and parental communications	4 hours	No
SEND Data	EHCPs	4 hours	No
	CINs	4 hours	No
Conduct and Behaviour	Exclusions, past and current	2 weeks	No
	Behavioural observations, staff notes and incident records	4 hours	No
Governance	School Improvement Plans	2 weeks	No
	Policies and procedures	4 hours	No
	Governor meeting dates	2 weeks	No
	Governor attendance and training records	2 weeks	No
	Governors minutes and agendas	2 weeks	No
Administration	Admissions information	4 hours	No
	School to school transfers	2 weeks	No
	Transition information	2 weeks	No
	Contact details of pupils and parents	4 hours	Yes – Emergency Grab Bag
	Access to absence reporting systems School diary of appointments / meetings	4 hours	No
	Pupil timetables	4 hours	No
	Letters to parents / newsletters Extra-curricular activity timetable and contacts for providers	4 hours	No

	Census records and statutory return data	4 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	Yes – Emergency Grab Bag
Office Management	Photocopying / printing provision	4 hours	No
	Telecoms – school phones and access to answerphone messages ~email – access to school email systems	4 hours	No
	School website and any website chat functions / contact forms	4 hours	No
	Social media accounts (Instagram) Management Information System (MIS) - Arbor	4 hours	No
	School texting messaging system – Arbor School payments system (for parents) – Arbor	4 hours	No
	Financial Management System – access for order / purchases (RM Unify)	4 hours	No
Site Management	Visitor sign in / sign out CCTV access	4 hours	No
	Site maps Maintenance logs, including legionella and fire records	24 hours	No
	Risk assessments and risk management systems	24 hours	4 hours No
	COSHH register and asbestos register	24 hours	Yes – Hard copy
Catering	Contact information for catering staff	4 hours	Yes – Emergency Grab Bag
	Supplier contact details Payment records for food & drink	4 hours	Yes – Emergency Grab Bag
	Special dietary requirements / allergies	4 hours	Yes – Emergency Grab Bag
	Stock taking and orders	24 hours	No

11. Training and Awareness

- **Cyber Security training** to be completed by all staff who use the MIS (Management Information System) Arbor as part of their daily routine.
- All staff with complete cyber security training as part of the GDPR In-House Training and Quiz completed annually or as a new starter.
- Regular updates and reminders on safe digital practices

12. Policy Review

This policy will be reviewed annually or following a significant cyber incident.

APPENDIX A: Incident Impact Assessment

Use this table to assess and document the scope of the incident to identify which key functions are operational / which are affected:

Operational	No Impact	There is no noticeable impact on the 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 the school has been 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 partis [Department of 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 Closed

Dear Parent/Carer,

I am writing to inform you that it appears the school has been victim of [a cyber-attack / serious system outage]. This has taken down the school IT systems. This means that we currently do not have 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 Commissioner Officer (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 pupils on [XXXXXXXXX]. We are currently planning that the school will open as normal on [XXXXXXXX].

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.

We will be working with the Location Authority, IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and re-open as soon as possible.

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

Yours sincerely,

3. Staff Statement Open

Amwell View 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 Amwell View School will remain open with the following changes to working practice:

[Detail any workarounds / changes]

We are 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. We have taken immediate action to mitigate data loss, limit severity, and restore systems.

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

4. Staff Statement Closed

Amwell View 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 Amwell View School will close to pupils [on DATE or with immediate effect]:

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

We are in contact with our Data Protection Officer and we have reported the incident to the ICO, 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. We have taken immediate action to mitigate data loss, however we are unsure when systems will be restored. Staff will be kept informed via [telephone / email / staff noticeboard].

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

5. Media Statement

Amwell View School 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.

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 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	Person Responsible	Completion Date		Comments	Outcome
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					

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:		