ACET IT / Cyber Protection Policies

ACET Cyber Security Policy

ACET Disaster Recovery Policy

ACET IT Incident Management Policy

DOCUMENT CONTROL		POLICY LEVEL Trust	
APPROVED BY	Audit & Risk Committee	APROVED DATE	22.07.24
BUSINESS LEAD	Network Leader	AUTHOR	Matthew Sutton
NEXT REVIEW DATE	September 2025	FREQUENCY	

VERSION NUMBER	DATE ISSUED	UPDATED INFORMATION
V 1.0	28.09.2022	First published version
V 1.1	02/08/2023	ICT Management Team Contact Details updated
V 1.2	26/06/2024	ICT Management Team Contact Details updated. **ACET DISASTER RECOVERY POLICY – 4.3 updated to make explicit that actions are post incident and analysis.** Cyber Response Checklist updated to emphasise isolation of devices as first response, and remove “pay ransomware demand” as potential remedial action.

ACET CYBER SECURITY POLICY

1. Purpose

This Cyber Security Policy outlines the Trust's guidelines and provisions for preserving the security of data and the technology infrastructure against a cyber-attack.

The more we rely on technology to collect, store, and manage information, the more vulnerable the organisation is to severe security breaches. Human errors, hacker attacks and system malfunctions not only cause great financial damage but also affect business continuity, compromise our GDPR compliance and can adversely affect our reputation.

For this reason, the Trust has implemented a number of security measures and instructions to help mitigate security risks.

2. Scope

This policy applies to all employees, contractors, volunteers, and anyone who has permanent or temporary access to systems and hardware.

3. Policy Principles

All measures laid out herein are designed to mitigate the effects of cyber threats on:

- The ability of the Trust to deliver services to schools
- The ability of schools to fulfil their teaching and learning responsibilities
- The security and integrity of confidential information
- Personal information on students, carers, staff, teachers etc.
- Unpublished financial information
- Intellectual property

There is an obligation on all staff within the trust to ensure data and systems are protected in line with the provisions laid out in this policy.

4. Policy Elements

4.1 Device management and protection

When staff use their digital devices to access systemic information, such as email or files, they introduce risk to the security of the systems. We therefore require all staff to maintain security on devices used to access such systems by adhering to the following conditions:

- Ensure all devices are secured with a password, PIN, or biometric access process
- Ensure the presence of Trust approved anti-malware (including virus) software on any device
- Always ensure the physical security of devices (e.g. not left on display in a car)
- Only use secure networks to connect to Trust services (e.g. using a VPN if on public Wi-Fi)
- Never disclose or share passwords

Staff should never share or loan their devices.

Any loss or new requirement should be raised with the ICT Team. This also applies if it is suspected that passwords or other credentials have been compromised.

Individuals will receive this policy on joining the Trust and should request clarification on any points they do not sufficiently understand.

4.2 Safe use of email

Malicious email is the primary vector of ingress to compromised networks. Therefore, good email discipline and hygiene should be maintained around the use of the Trust's email systems and facility.

Good practices include (but are not limited to):

- Be suspicious of any email with an attachment or which includes links
- Verify the sender is as expected, and any attachment is also expected
- Check links are spelled correctly, and do not hide their true destination (hovering over link text should show the actual target)
- Never open any attachment, or click on any link, of which you are unsure
- Be wary of any email saying a file has been shared with you. Confirm this (verbally if possible) with the sender of the email
- Be wary of an email which says it contains a voicemail. Confirm this with ICT before clicking links or opening attachments

If a staff member is not sure that an email they received is safe, they must refer this to the ICT Department. Suspicious emails should never be forwarded as this can spread a virus. Further guidance can be found in the Trust E-Safety Policy.

4.3 Authentication management (passwords)

Authentication integrity is a key component of the security of ICT Systems. This includes (but is not limited to) passwords, PIN codes, passphrases, biometric data and cryptographic certificates. In all instances these should be treated as highly confidential.

Strong discipline is encouraged when choosing authentication security. Wherever possible multi-factor authentication should be utilised to mitigate the risk of any one credential being compromised.

Passwords, PINs and passphrases should be as secure as possible, and should be memorable so as not to require the user to store this information in an accessible form anywhere.

Password length is a key to good security. For example:

"This is my passphrase and I remember it every day" is substantially more secure than "4^jsyR&f", due to the length as well as being easy to remember.

4.4 Secure data transfer

Transferring data introduces security risk. It is, however, necessary (e.g., to exam boards). As such, Staff must:

- Avoid transferring sensitive data (e.g. pupil information, reports or marking sheets) to other devices or accounts unless necessary
- Only share confidential data over the Trust's network (including VPN) and not over public Wi-Fi
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies
- Ensure any email attachments containing personal or confidential data are password protected and ensure that the password to open an attachment is not included in the e-mail (ideally sent via a second channel such as SMS)
- Report scams, privacy breaches and hacking attempts.

In all cases the ICT Team will offer support if requested.

4.5 Additional measures

The ICT Team must be made aware of any perceived threat, suspicious activity, or phishing attack. This should be via the usual channels but should be flagged as a cybersecurity concern to ensure appropriate escalation.

The following behaviours are strongly encouraged:

- PCs and Laptops should always be locked when left unattended, and the screen turned off
- Report to ICT the presence of any discovered, unexpected, or unexplainable ICT hardware
- Report to ICT any perception of a weakness in the Trust's cybersecurity
- Avoidance of non-work-related web activity on Trust networks, even during breaks

The ICT Team will always respond to cybersecurity threats, information or risks urgently, with a pre-defined escalation route being observed.

It is incumbent on the ICT Team to architect services and systems for security, including:

- Firewalls, VPNs, filtering, monitoring and ACL management solutions
- Regular training and briefing notes about new threats and horizon risks
- Responding to any reported cybersecurity incident urgently

5. Policy breaches

It is expected that all employees follow this policy. Any breach of this policy will be treated extremely seriously and may lead to disciplinary proceedings.

Limitations of this Policy

While every endeavour is made to secure the ICT systems, the nature of exploits and malicious actors is such that it is possible a route may be found to breach the security of the systems. In this case, and ICT Cyber security incident is declared, and the Incident Management process invoked.

ACET DISASTER RECOVERY POLICY

1. Purpose

The aim of Aston Community Education Trust ("the Trust") is to ensure all data and information stored electronically on its systems is recoverable in the event of a disaster incident. This policy defines the mechanisms by which such recovery is made possible and sets out a schedule for testing to ensure that the efficacy of this process is exercised, and the results recorded.

2. Scope

The Trust employs a common technology across all school sites to provide a homogenous backup and recovery solution. Servers on all sites are backed up locally, and copies of these backup images transmitted securely to either an in-house 'cloud' storage solution or off-site replication via the proprietor's appliance. This policy covers servers and services managed using this technology.

Data and documents stored in cloud services such as Office 365 and Google Workspace (formerly G Suite) are outside the scope of this policy. Whilst it is important to consider backing up this data, there are already tools intrinsic to these systems to provide short term data recovery. This policy covers the essential infrastructure that underpins daily operations within the academies.

3. Policy Principles

This policy is designed to outline the technology used to protect the Trust's data, and to describe a top-level recovery operation. The technical steps required to actuate the recovery are detailed in a separate work instruction document aimed at technically competent ICT engineers.

A disaster incident may be a physical incident impacting on the ability of the information systems to deliver the services and data on which the Trust relies, it may be a cyber security incident compromising the systems and rendering the services inoperable, or it may be an infrastructure failing which precludes the ability of the systems to deliver the services. The systems and service recover process is the same regardless of the disaster incident type, only the target recovery location of hardware may vary.

Service recovery is defined by, and measured in terms of, recovery times and points. The objective of the Trust ICT Team is to have the Recovery Point Objective (RPO) as low as possible, and as close to real time as is feasible, and the Recovery Time Objective (RTO) as short a period after the disaster event as possible.

3.1 Definitions

Recovery Point Objective (RPO): The recovery point objective is the point to which information used by an activity must be restored to enable the activity to operate on resumption. RPO can also be referred to as 'maximum data loss'.

Recovery Time Objective (RTO): The recovery time objective is the maximum amount of time allowed to resume an activity, recover resources, or provide products and services after a disruptive incident occurs. This target time period must be short enough to ensure that adverse impacts do not become unacceptable.

Source: ISO 22301:2012

4. Policy Elements

The backup and recovery technology of choice used by the Trust is Barracuda and Veeam Backup & Replication. The architecture of the backup solution is shown below in figure 1. The guiding principle that governs the backup strategy is the 3-2-1 approach: 3 different backups, located in at least 2 places and 1 held offsite. The current configuration is to backup servers nightly, and replicate offsite nightly, giving RPO of less than 24 hours.

The processes to be carried out in identifying a disaster recovery incident are documented in a separate policy:

ACET IT Incident Management Policy

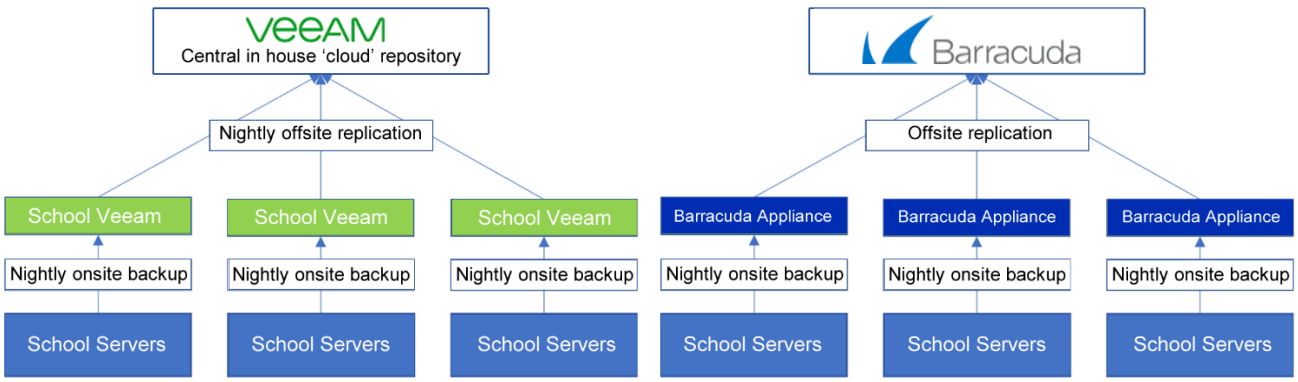


Figure 1. Backup architecture

4.1 Crisis Team

In the event of a disaster recovery scenario, a crisis team should already have been convened through the IT Incident Management (IM) process. This team should, throughout an incident, be engaged in disaster recovery activities, and tasks assigned by the crisis lead as required.

For convenience, the ICT crisis team should consist of the ACET Network Manager for the Trust, who will co-ordinate the technical recovery with the Assistant Network Manager and Senior Technician(s), maintain strategic oversight, authorise changes as required, and ensure the communications plan is followed.

Key stakeholders for each school have been identified via the Business Continuity Plan and will form the school contingent of the crisis team, along with any nominated other.

Contact details for the ICT team are contained in Appendix I.

4.2 Server Recovery

The virtual nature of most servers within the Trust estate means that the loss of one physical host due to a physical incident such as fire, flood or malicious damage is easily surmounted. The following is the general process necessary to recover a server:

- Log on to the local recovery server, or cloud storage area
- Right click and select “Restore” from the menu
- Navigate the resource tree and locate the server(s) required
- Restore the required object (VM or File/Folder)

4.3 Cybersecurity incident

Recovery from a cybersecurity incident is handled in the same manner as from any other incident, with the caveat that, post incident resolution and analysis, the ICT team must ensure that target hardware is factory reset and / or bare metal installation, to eliminate the risk of any low level firmware rootkit malware. An internal IT department “Cybersecurity Response Checklist” (appendix III) document will be used to clarify roles in such an event and direct members of IT Technical Staff to ensure a swift and efficient response.

5. Communications Plan

In the event of a disaster recovery incident, the ICT lead will refer to the ACET Business Continuity Plan and its contents for the communication plan and surrounding roles.

6. Scheduling and Exercising

The efficacy and viability of recovering servers and services from backup and DR provision must be validated and recorded via a managed and monitored schedule of tests across the Trust recovery estate. This is a responsibility of the ICT Team, in conjunction with key stakeholders in the school, to arrange and carry out per schedule. Each school must be tested at least annually.

The schedule and results of exercises are maintained in the document:

ACET DR Schedule.xlsx **(appendix II)**

Limitations of this Policy

This policy defines the overall architecture recovery paradigm of the Trust. Where schools have implemented systems or services outside of the purview of the ICT team, no responsibility is taken for the recoverability of these solutions. All new services and solutions should be implemented with the ICT team and requirements for recoverability captured as part of the project process. These solutions will then be added to the DR testing schedule.

Appendix I

ICT Management Team contact details

Name	Main Site	Email	Phone
Matthew Sutton	ACET (Trust Wide)	matthew.sutton@astoncetrust.org	-
Jamie Finch	ACET (Trust Wide)	jamie.finch@astoncetrust.org	-
Luke Rotherham-Fairclough	Swinton Academy	luke.fairclough@astoncetrust.org	-
Joe Davis	Aston Academy	joe.davis@astoncetrust.org	-
Adam Turner	Aston Academy	adam.turner@astoncetrust.org	-
Tasawer Iqbal	Swinton Academy	taz.iqbal@astoncetrust.org	-
Raeese Jamshaid	Aston Academy	raeese.jamshaid@astoncetrust.org	-
Andy Lowery	Shirebrook Academy	alowery@shirebrookacademy.org	-

Appendix II

Example ACET DR Schedule.xlsx

ACET - Disaster Recovery Testing

This schedule and list of results must be maintained by the ICT Team to accurately record dates and results of testing carried out in accordance with the schedule.

Complete the below accurately. Any failures must be documented on the 'Failures' tab, along with follow-on actions and re-testing schedule.

Test ID	Schedule Date	School	Actual Date	Server(s) recovered	Start time	End time	Duration	Technician	Success	Notes / observations
1	19/05/2022	LDJA	19/05/2022	LDJA-FPS	15:23	15:36	13mins 30	NB	N	No backups available on Veeam, attempted through Barracuda but failed.
2	23/06/2022	AH	23/06/2022	AH-FPS	09:57	11:01	1hr 4mins	NB	Y	No backups available on Veeam, done from Barracuda
3										
4										
5										
6										
7										
8										
9										
10										

Appendix III

Cybersecurity Response Checklist

Priority	Remedial Action	Persons Involved	Description
1	**Isolate** Systems	MSU	Upon first discovering of a ransomware attack, identifying and isolating infected devices key to stopping or slowing the spread.
		Senior Techs	Disconnect from the network any identified infected PC's
		1st & 2nd Line Techs	Disable the WiFi
			Disconnect from the network any servers where there may be mapped drives\shares to critical data (detach from Virtual switch)
1a	Communicate to SLT	JFI	Update nominated Business Continuity Plan representative as to what is happening
		(or alternate if not on site)	BCP Rep, RSc, RHi, SLT of any affected academy(ies)
2	Determine scope of infection	MSU & Senior Techs	Checked mapped drives, shared areas, network storage, online storage all for signs of encryption/infection
3	Determine if data/credentials stolen	MSU & 1st & 2nd Line Techs	Check log files. Look out for zip files as staging locations. Check for malware tools. Check for messages from perpetrators
2a & 3a	Determine strain of ransomware	JFI	Determine strain of ransomware and if there are any remediation tools available
		Tools	https://id-ransomware.malwarehunterteam.com/, https://www.nomoreransom.org/en/index.html
4	Determine appropriate course of action	All stakeholders	- Restore files from backups
			- Try to decrypt files
			- Any restorative action needed?

ACET IT INCIDENT MANAGEMENT POLICY

1. Purpose

The aim of the Aston Community Education Trust ("the Trust") is to respond efficiently and successfully to all ICT incidents, to mitigate downtime and loss of resource as a result of incidents, and to effectively involve third parties to assist in incident resolution where required.

2. Scope

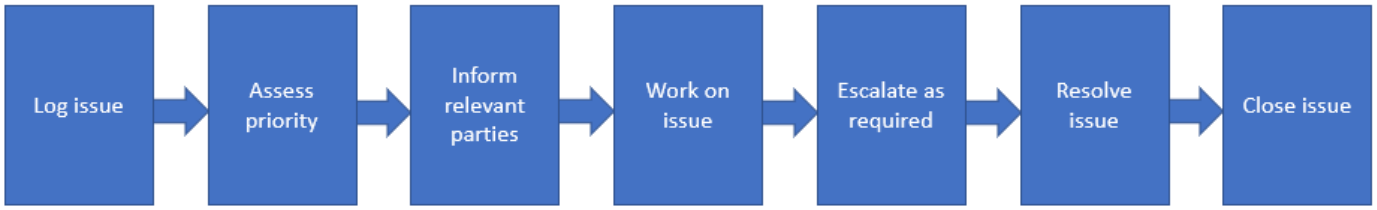
This policy endeavours to define the actions to be taken to triage possible incidents into categories of minor, medium, severe and cyber incidents, and to define the steps to be taken in each case to mitigate the effects of the incident. This includes all incidents affecting IT Service provision within the Trust, however incident resolution options are limited for third party hosted solutions, and management rather than technical resource may be required.

3. Policy Principles

This defines the Incident Management (IM) process in use at the Trust. All service affecting issues are treated as incidents and managed as according to the processes laid out herein.

4. Policy Elements

The basic workflow for managing incidents is the same regardless of severity, and can be characterised as follows:



The contents of each step will vary depending on the incident, its severity, and dependencies. Incidents are categorised as minor, medium, severe, and cyber. All cyber incidents are treated as severe.

4.1 Incident triage and severity

On receipt of initial alert to a potential incident, the receiving technician must ascertain the severity of the issue. Severity can be defined from the below matrix, although this does not provide for every scenario, and some judgement is required from the technician.

It is allowed that it is better to assign too high a severity than too low. All cyber incidents must be treated as severe.

No. of users affected	Geography affected	Potential damage	Severity
1-10	Single school	Minor loss of functionality, delay to email	Minor
10-30	Schools in local area	Wider functionality loss, lack of services, remote working impacted	Medium
30+	All Trust schools	Data loss, downtime, reputational damage,	Severe

		school closure, major impact on T&L	
Cyber	-	Data loss, downtime, reputational damage, school closure, major impact on T&L	Severe

4.2 Minor incident workflow

The minor incident (MIN) workflow may be managed solely by a single technician, and not require escalation – technical or management.

The MIN may become escalated to a medium or severe incident if further developments mean the scale and scope widens. At this point the relevant people should be informed per the workflows for those severities.

The MIN workflow can be characterised as follows:

- Ticket raised and logged on ticketing system
- Incident details ascertained, and contact with reporting user made
- Work on requirements, resolve issue
- Communicate resolution to user
- User confirms resolution, close ticket OR user disputes resolution, ticket remains open for further work.

4.3 Medium incident workflow

The medium incident (MEN) workflow requires that the responsible Senior ICT Technician be made aware of the incident and kept up to date with developments. The Senior ICT Technician is responsible for managing the incident at a technical level and ensuring the actioning technician has the required technical support to resolve the issue. Should further

management escalation be required, the Senior ICT Technician should inform the ACET Network Manager who will make decisions on how to progress.

A MEN may require the Senior ICT Technician to assist the technician; it may mean invoking support contracts to engage third party support; it may mean invoking the backup / disaster recovery process; it may mean requisitioning additional resource from within the Trust ICT Team. It is the responsibility of the Senior ICT Technician to inform the ACET Network Manager should further resource be required, or if resource is likely to be required outside of normal working hours.

The MEN workflow requires that a communication be issued to affected users periodically throughout the course of the incident to advise one of the follow statuses: *incident acknowledged; work ongoing; incident resolved.* It is acceptable to repeat the status "work ongoing" several times to reassure stakeholders that work is, indeed, ongoing.

The MEN workflow can be characterised as follows:

- Ticket raised and logged on ticketing system
- Incident details ascertained, and contact with reporting user made
- Escalate to Senior ICT Technician and issue initial communication to stakeholders ("*incident acknowledged*")
- Work on incident
- Escalate via technical or management route to acquire required resources
- (Re-)issue communication to stakeholders ("*work ongoing*")
- Continue work on incident with additional resources
- Resolve issue
- Communicate resolution to user ("*incident resolved*")
- User confirms resolution, close ticket OR user disputes resolution, ticket remains open for further work.

A medium severity incident may merit follow up review and lessons learned assessment. This should be decided by the Senior ICT Technician in conjunction with the ACET Network Manager and scheduled accordingly.

4.4 Severe incident workflow

The Severe Incident (SIN) workflow requires that **all** Senior ICT Technicians and the ACET Network Manager be informed immediately of the incident as soon as anyone becomes

aware of it. This is likely to follow that the discovering technician will alert their Senior ICT Technician, who will alert the remainder of the team.

The SIN workflow differs from the MEN workflow in that the ACET Network Manager will urgently advise key stakeholders within the Trust of the developing incident, with a view to mitigating non-technical aspects that may arise from the incident.

In a SIN situation, the ACET Network Manager will co-ordinate mitigation and recovery efforts. Communications must be issued to keep key stakeholders updated, regardless of whether it is an internal (i.e. a Trust systems) issue, or an external (e.g. power outage) issue. All resolution options should be considered, including disaster recovery, additional site usage, and third party assistance.

The SIN workflow can be characterised as follows:

- Ticket raised and logged on ticketing system
- Incident details ascertained, and contact with reporting user made
- Escalate to ACET Network Manager and Senior ICT Technicians and issue initial communication to stakeholders
- ACET Network Manager co-ordinates with SLT across Trust functions to updates and manage response
- Work on incident
- Escalate via technical or management route to acquire required resources
- (Re-)issue communication to stakeholders ("*work ongoing*") with suitable amount of detail for SLT update
- Continue work on incident with additional resources
- Resolve issue
- Communicate resolution to user ("*incident resolved*")
- User(s) confirms resolution, close ticket OR user disputes resolution, ticket remains open for further work.

A severe incident **must** be followed up with a subsequent review and lessons learned assessment. The ACET Network Manager will own this process and report back to Trust SLT on outcomes.

4.5 Cyber (severe) incident workflow

In the event of a cyber incident (CIN) being declared, the SIN workflow should be followed but the key initial stage should be to **isolate** the affected machine(s) from the rest of the network as quickly as possible. Once removed from the network, forensic analysis can be carried out to determine the type and scope of the incident.

Removing infected machines from the network may involve powering off switches, removing patch cables or powering down machines. This should be done as soon as possible to limit the spread of the incident.

The SIN workflow should then be invoked and followed while the incident is managed.

Limitations of this Policy

This analysis document is for information gathering and should be used in conjunction with the ACET Disaster Recovery policy and local site work instructions to inform the recovery process.