Bright Futures
EDUCATIONAL TRUST
The best *for* everyone, the best *from* everyone

Cyber Security Policy

Date of Policy Approval:	November 2021
Owner of Policy:	Digital Technologies Manager
Authorised By:	Executive Team
Policy Review Date:	November 2023
Distribution:	All Trust Staff All Members/Trustees/ Governors Consultants working on behalf of the Trust Websites

This is a Trust-Wide Policy.

Bright Futures Educational Trust's (Bright Futures or the Trust) Strategy underpins all aspects of this policy and the way in which it will be applied. These elements are:

- Our vision, the best for everyone and the best from everyone;
- Two of our values; Integrity: We do the right things for the right reasons and Passion: We take responsibility, work hard and have high aspirations;
- Two of our commitments: Effective Communication and Strong Governance and Accountability.

What is the Policy For?

Bright Futures Educational Trust ("the Trust") is obliged to ensure that all its Information Technology (IT) Systems are secure and not subject to improper use. This policy describes the responsibilities for all users, including those of privately owned devices that connect to Trust systems.

The purpose of this policy is to protect the Trust's devices and data from cyber-attack.

Cyber-attacks can lead to systems becoming unavailable, data loss, financial loss and reputational damage, Implementation of this this policy reduces the likelihood of these effects.

This policy encompasses guidance from internal audit recommendations, the National Cyber Security as well as the Academy Trust Handbook 2021.

This policy should be read in conjunction with our

- Password Policy
- Combined Data Privacy Policy
- E-Safety Policy

Who is the Policy for?

This policy is for the attention of anyone who is employed by, provides a service to, or volunteers to work at Bright Futures and uses its IT systems either on a Trust owned device or a personally owned device. This includes governors and trustees.

This policy is split into two sections. Section 1 is for all users and provides a non-technical explanation of the key elements of cyber security. It is contained in pages 2 and 3.

Section 2 of the policy covers the same key elements in more technical detail and is intended for Bright Futures' IT staff and workers. This section starts on page 4 and continues for the remainder of the document.

SECTION 1: Cyber Security for all users

Firewalls
A firewall is a device or software program that is located between your computer and the internet. It manages data flowing to and from your device, allowing legitimate connections and blocking malicious ones.

If you are using a Bright Futures' computer, you are always protected by a firewall that is managed by the IT Department.

If you suspect your firewall is not working or incorrectly blocking a service, please contact the IT Department for help. it@bfet-support.co.uk

Endpoint Protection
Endpoint Protection or Antivirus software when Installed on a computer, scans for malicious software such as computer viruses, malware or ransomware. This protects your computer and data from malicious damage or theft.
If you are using a Bright Futures computer, it will already have Endpoint Protection installed, this is managed by the IT department.

It is important that Endpoint Protection software is up to date so that it can protect against the very latest threats. If you suspect the protection on a device is not up to date, please contact the IT department.

If you encounter a message that a device is infected with a virus or you suspect it is, turn it off and contact the IT department immediately. it@bfet-support.co.uk

Updates and Patches
Security vulnerabilities that enable malicious activity on computer systems are discovered frequently, software companies release security updates and patches on a regular basis. These must be installed to ensure devices have the latest protection. Out of date software increases vulnerability to cyber threats.
The IT Department ensure that all Trust devices are updated in a timely manner.

Remote Working
Remote working accessing Trust systems from external locations. This could be from home, another school or a public place. If you are connecting to a network that it not managed by the IT department you should be aware that it could be less secure.
Devices supplied by Bright Futures will still be protected by a firewall and antivirus software while working remotely.

You must only work remotely through the secure methods provided by the IT department such as Office 365 or Remote Desktop.

You must also only work on data where it is stored, on secure Trust systems rather than downloading it to your device for editing.

You should be aware of your surroundings when working on sensitive data or entering passwords and beware of 'shoulder surfers'.

Bring Your Own Device (BYoD)

Some users prefer to use their own IT equipment for either working remotely or bringing your own device into work. This is permitted but does require you to take some steps to protect your device and Trust systems as security precautions normally managed by the IT department are the responsibility of the device owner.

You must ensure you have a firewall enabled to protect against unauthorised access to your device and the systems to which it is connected. Most computer operating systems include a firewall as do many internet routers supplied by ISPs. A number of third-party options exist.

You must ensure you have an up-to-date antivirus software installed. Some operating systems have one built in, there are several free, third-party options available as well.

Your device must have up to date software that is still under support and receiving security updates. The latest updates and patches must be installed.

If you require advice on enabling a firewall or antivirus protection or installing security updates the IT department can help with this.

If you share a device with other people, such as family members you must take steps to ensure they do not have access to trust data.

You should only access trust data where it is stored, you should ensure you work with data directly on a secure platform such as Office 365 and do not download it to your device.

When in a Trust school or office you should only connect to a dedicated BYoD network which is provided by the IT Department. Personal devices cannot be connected to the school network. The IT department can assist you to get connected to the correct network. Please contact it@bfet-support.co.uk

Passwords

Passwords are an effective security countermeasure if they are strong and kept confidential. Passwords are a means of validating a user's identity to access a computer resource, to ensure the security of that resource and to maintain the confidentiality of information held on that resource. In most cases systems will have settings to ensure you choose a password that is secure. When selecting a password, it is important that you chose a password that is hard to guess and easy to remember, you should avoid using the same or variations of the same password.

Cyber Security Incidents

A cyber security incident is a breach of a computer system, there are a number of forms of cyber incident, it could be a virus infection, someone having access to data that they should not be able to access, a phishing attempt or a complex cyber-attack that causes a system to be unavailable.
All users have a responsibility to report cyber incidents. If you become aware of a cyber incident or a situation that you suspect could be an incident, you should report this immediately to cyber@bright-futures.co.uk.

SECTION 2: Cyber Security for IT technical staff

Content

Firewalls

Firewalls are implemented for the purpose of securing the trust's IT infrastructure and devices from each other as well as external threats.

The term Firewalls may refer to both physical hardware firewalls and virtual software-based firewalls.

Firewalls work by being situated between networks where all traffic leaving and entering the protected network must flow through the firewall. The firewall will inspect the traffic and use configured rules and polices to make decisions as to whether traffic is allowed or blocked.

Networks can be considered Trusted or Untrusted. Trusted networks are networks that are owned and managed by the Trust. Untrusted networks are networks that are not owned or managed by the trust such as a user's home network, a network in a partner organisation or public network.

- All points where trusted networks connect to the untrusted networks must be protected by a firewall.
- All firewalls must have intrusion prevention (IPS) enabled for additional security.
- Administrative access to firewalls must be protected with a form of multi-factor authentication.
- All firewalls that are positioned between trusted networks and untrusted networks must be configured so that the IT department is alerted to any configuration changes.
- All trust owned computers must be protected with a software firewall when connected to trusted and untrusted networks.
- Firewall configurations will adopt a 'least privilege' approach and should limit traffic to only that which is needed.
- Firewall rules must be documented in a secure central location. Configurations will be periodically reviewed to ensure they meet the Trusts requirements and current security best practice.
- Firewall logs will be actively monitored, and any breach or suspicious behavior will be treated as a cyber security incident.
- Changes to firewall rules must be requested via the IT Service Desk and subjected to change management procedures prior to being implemented.

Endpoint Security

Endpoints are the devices that connect to the Trust's networks such as desktops, laptops or servers, these may be Trust owned devices or personal devices. These devices are all potential entry points for cyber-attacks, vulnerabilities in endpoints represent a risk to Trust systems.

The term malware is used to describe different types of malicious software including, viruses, ransomware, trojans, mail bombs and root kits. The effects of this software can be damage to or theft of data, make IT systems unavailable and precipitate further cyber-attacks both inside and outside the Trust.

There are many sources of malicious software including websites, email, portable storage devices or infected personal devices that connect to Trust networks.

The impact of malware infection is a serious risk. Access to systems and data may be disrupted for extended periods during an infection while the infection is cleaned, and data restored. There may be financial impact and reputational damage due the infection in relation to data breaches.

- All trust devices must have an anti-malware product installed that is up to date and continuously monitors for malware. This product must report back to a management console where the IT department can monitor it.
- All Trust owned devices will be supplied with an appropriate anti-malware product that will be maintained by the IT department.
- All devices connected to the trust network must run a supported version of their operating system and installed applications with the latest available patches applied.
- Anti-Malware software must be configured for on-access scanning which must include downloading or opening of files and folder and web page scanning.
- Anti-Malware must be configured to run regular system scans at least once daily.
- Email attachments must be scanned for malware prior to delivery.
- Users should consider the authenticity of email attachments and internet file downloads prior to opening them
- Users must be prevented from accessing known malicious websites using a content filtering system.
- Users must not disable anti-malware software, any on screen messages suggesting that anti-malware is disabled or not functioning should be reported to the IT department.
- Anti-malware must not be configured to bypass or exclude any files or folders, in specific cases where this is necessary such configuration must be carried out by the IT Department and would be subject to change management procedures.
- Users experiencing difficulty with anti-malware installed on trust owned devices should seek technical support from the IT department.
- The IT department reserves the right to disconnect any device from Trust systems where an infection is found or suspected. The device will remain disconnected until the infection has been removed.
- If you suspect a device is infected with malware, report the incident to the IT department as soon as possible.

Patch and Vulnerability Management

In order to protect the Trust's IT systems from vulnerabilities and ensure ongoing and consistent operation it is important to adopt a managed approach to regular installation of patches, updates and firmware to devices, operating systems and applications. Regular updates are critical to maintaining a secure and operational environment. All devices connected to Trust networks require regular patching.

Vendors rate patches on a scale dependent on the severity of the vulnerability or issue that the patch addresses. This may be vendor specific or use a standardized model such as the Common Vulnerability Scoring System (CVSS).

The Trust uses a Vulnerability management tool to scan a sample of devices for known vulnerabilities that require remediation. Vulnerabilities found will be added to the vulnerability register and action will be taken to remediate the vulnerability.

The Trust uses a third-party patch management solution which is part of its Remote Management and Monitoring Software (RMM). This software works by installing a software 'agent' onto a device, this agent then communicates with the RMM management tool. This product manages Windows and Apple MacOS endpoints.

- The IT Department will ensure they receive regular notifications from software vendors when patches become available where possible. Weekly automatic update reports from the RMM will also be used to identify required patches. Where automatic updates are not available manual checks will be made on a regular schedule.
- Schools may use a Windows Server Update Services (WSUS) server to centrally hold copies of patches to alleviate impact on internet connections during patch downloads. These servers must only be acting as patch repositories and not be configured to manage patches. This aspect is controlled by the RMM tool.
- The RMM agent must be installed on all Trust owned endpoint devices. Users must not be able to disable or remove the RMM agent.
- All updates and patches will be tested prior to deployment on test endpoints. Where there is no suitable test endpoint available, patches will be applied to a non-critical production device which will then be monitored prior to the wider release of the patch.
- Patches that are rated as critical or high risk by the vendor must be deployed within 14 days of release.
- Patches that are rated as medium, low or carry no severity must be deployed within 28 days of release.
- In the absence of a vendor rating category the table below can be used to assess and categorize the rating of any identified vulnerability.

Rating	**CVSS Score**
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

- Devices that are not compatible with the RMM agent for example Linux servers must be documented and checked on a weekly basis, with patches applied to the timescale above.

- All mobile endpoints such as iPads and Android tablets owned by the trust should be joined to a Mobile Device Management Platform (MDM) that has the capability to detect and deploy patches
- Patches may only be downloaded from the authorized vendor and not from third-party sources.
- Software that has fallen out of scope for vendor patches and is therefore no longer supported must be removed or updated to a version that is supported.
- Hardware that is only able to run unsupported operating systems and software must be removed from Trust systems and disposed or upgraded.

Remote Working

Remote working is the process of accessing Trust IT systems via any network that is not owned and managed by the Trust. This may include working from home, visiting the offices of other schools or partner organisations and working from public networks such as conference centers, hotels or cafes

Remote working poses additional risks to cyber security. Accessing systems via untrusted networks means that users can be more vulnerable to cyber-attacks. Users must at all times, consider the additional risk

- When working remotely users' devices must be protected by a firewall. Devices supplied by the trust for remote working will be issued with a software firewall installed.
- Users accessing trust data via a personal device must ensure they supply their own firewall.
- Remote access to trust systems must only be carried out via a secure and encrypted connection. The IT Department will ensure that all public facing systems can only be accessed in this manner.
- All devices used for remote working either Trust owned, or personal devices must have anti-malware software installed and adhere to the requirements of the Endpoint Security section of this policy.
- Users should be aware of their surroundings and protect yourself against "shoulder surfing" and take extra care when entering passwords or viewing sensitive documents. This is of particular importance when working in public areas.

Client VPN (Virtual Private Network) is the process of using, via software, a secure private connection to a remote system. A client VPN places the remote device as if it were part of the trusted network. This poses additional security issues.

- Remote access to internal systems must only be achieved through either a remote desktop solution in or a client VPN.
- Client VPN software must be kept up to date and have all its latest security patches installed.
- Access to systems via a client VPN is only available via Trust owned devices. Personally owned devices are not permitted to use client VPN.
- Only the IT Department may set up VPN access to internal systems.
- Only named individual users should be granted VPN access to trust systems. These users should be recorded centrally along with the system to which they have access.

- VPN must be used in conjunction with network segmentation. VPN clients must be segmented from the rest of the network and only have access to the network segment where the services they require are located.

Bring Your Own Device (BYOD)

Whilst the trust does not require staff or students to use their own personal devices for work purposes it is recognized that it is often convenient and such use is permitted subject to the following requirements and guidelines.

- BYOD devices must connect to systems via a dedicated network either via a wireless network specifically configured for BYOD devices or a dedicated ethernet socket.
- BYOD devices must egress onto a dedicated network segment and not become part of the trusted network.
- Users are not permitted to remove ethernet cables from Trust owned devices in order to gain access to the network.
- The IT Department must ensure that unused ethernet sockets are either unpatched or place the device in a quarantined network with no access to any services.
- Where schools wish to permit BYOD devices access to resources on the trusted network this must be requested via the Digital IT Manager and subjected to risk assessment and change management procedures. A secure solution must be adopted to protect elements of the trusted network from risks associated with BYOD devices.

Users must at all times give consideration to the risks of using personal devices to access Trust information, in particular information that is classified as sensitive or confidential.

- The device must run a current version of its operating system. A current version is defined to be one for which security updates continue to be produced and made available to the device.
- Users should work on data directly at the source, for example documents should be opened from and saved directly back to Office 365. Data should not be downloaded to the local disk of the device.
- Where downloading of data to a device is unavoidable, devices must be encrypted. (Some older devices are not capable of encryption, and these should be replaced at the earliest opportunity.) Data considered as personal should not be downloaded to personal devices.
- A passcode/password must be set for all accounts which give access to the device.
- Users working remotely to access Trust systems on a personal device must ensure they have a firewall in place. See the remote working section of this policy for further guidance
- Devices must have an anti-malware product installed that is up to date and continuously monitors for malware. See the Endpoint Protection section of this policy for further guidance.
- A password protected screen saver/screen lock must be configured.
- The device must be configured to “autolock” after a period of inactivity (no more than 15 minutes).
- Devices must remain up to date with security patches both for the device’s operating system and its applications.

- The device security must not be compromised (e.g., by “jail breaking” or “rooting” a smartphone).
- All devices must be disposed of securely.
- Mobile devices must be enrolled in the Trust MDM to enable remote wipe of Trust data from the device.
- The loss or theft of a device containing Trust Data must be reported to the IT Department.
- Any use of personal devices by others (family or friends) must be controlled in such a way as to ensure that these others do not have access to Trust data.

In addition to the above requirements, the following recommendations will help further reduce risk:

- Consider configuring the device to “auto-wipe” to protect against brute force password attacks where this facility is available.
- Consider implementing remote lock/erase/locate features where these facilities are available.
- Do not leave mobile devices unattended where there is a significant risk of theft.
- Users should be aware of their surroundings and protect yourself against “shoulder surfing” and take extra care when entering passwords or viewing sensitive documents. This is of particular importance when working in public areas.

- Be mindful of the risks of using open (unsecured) wireless networks. Consider configuring your device not to connect automatically to unknown networks.
- If a personally owned device needs to be repaired, ensure that the company you use is subject to a contractual agreement which guarantees the secure handling of any data stored on the device.

Passwords

Passwords are an effective security countermeasure if they are strong and kept confidential. Passwords are a means of validating a user's identity to access a computer resource, to ensure the security of that resource and to maintain the confidentiality of information held on that resource.

For full guidance on passwords see the Bright Futures Educational Trust Password Policy

Cyber Security Incident Management

Definition of a Cyber Security Incident

A cyber–Security Incident is a breach of a system’s security in order to affect its integrity or availability, the unauthorised access to or attempted use of a system; or a breach of Trust IT Policies or procedures.

Examples include, but are not limited to:

- Loss of data or a device where such data is stored for example a laptop.
- Theft of a Trust owned device or personal device used to access Trust data.
- Unauthorized access to data.

- Breach of account credentials such as in a phishing attack.
- Unauthorised disclosure of information, such as email sent to an incorrect recipient.
- Malware infection.
- Disruption to systems caused by a cyber-attack such as a Denial of Service.

Responsibilities

It is the responsibility of all users of Trust IT systems to report any potential Cyber Security Incident.

Reporting and Analysing an Incident

All reports of a potential Cyber Security Incident should be made to the Digital IT Manager at the earliest opportunity by telephone or email. Users should include as much detail as possible, including:

- Date, time and location of the incident.
- Which systems and data are affected?
- What has happened?
- How was the incident discovered?
- What containment or recovery has already taken place?

The incident will be logged in the Cyber Security Incident Log and a lead investigator will be appointed.

The lead investigator along with the IT Department will analyse the incident, categorise it and assign it a severity using the matrixes in this policy.

The lead investigator will determine the extent of the incident. Where necessary the lead investigator will escalate the incident for appropriate oversight from senior management as well as liaising with other key stakeholders such as finance, HR or safeguarding where required.

In the event an incident requires reporting to a third party for example if a data breach is reportable under GDPR this will be done at this stage in line with any relevant Trust polices such as the Combined Data Privacy Policy.

Containment and Mitigation

The lead investigator along with relevant team members will determine the appropriate course of action required to limit the impact of the incident. This may involve action such as isolating specific networks or shutting down critical equipment.

Non-technical steps may need to be taken at this stage such as liaising with parents, partner organisations or the media.

Care must be taken at this stage of the incident to consider the impact of any actions. This is particularly relevant in live targeted attack scenarios where the responses of the attacker to any reactions from the Trust may escalate the incident.

Remediate and Eradicate

Steps at this stage of the response may be similar to those in the Containment and Mitigation phase. Action will be taken at this point to completely remove the cause of the incident and confirm that this has been successful.

Recovery

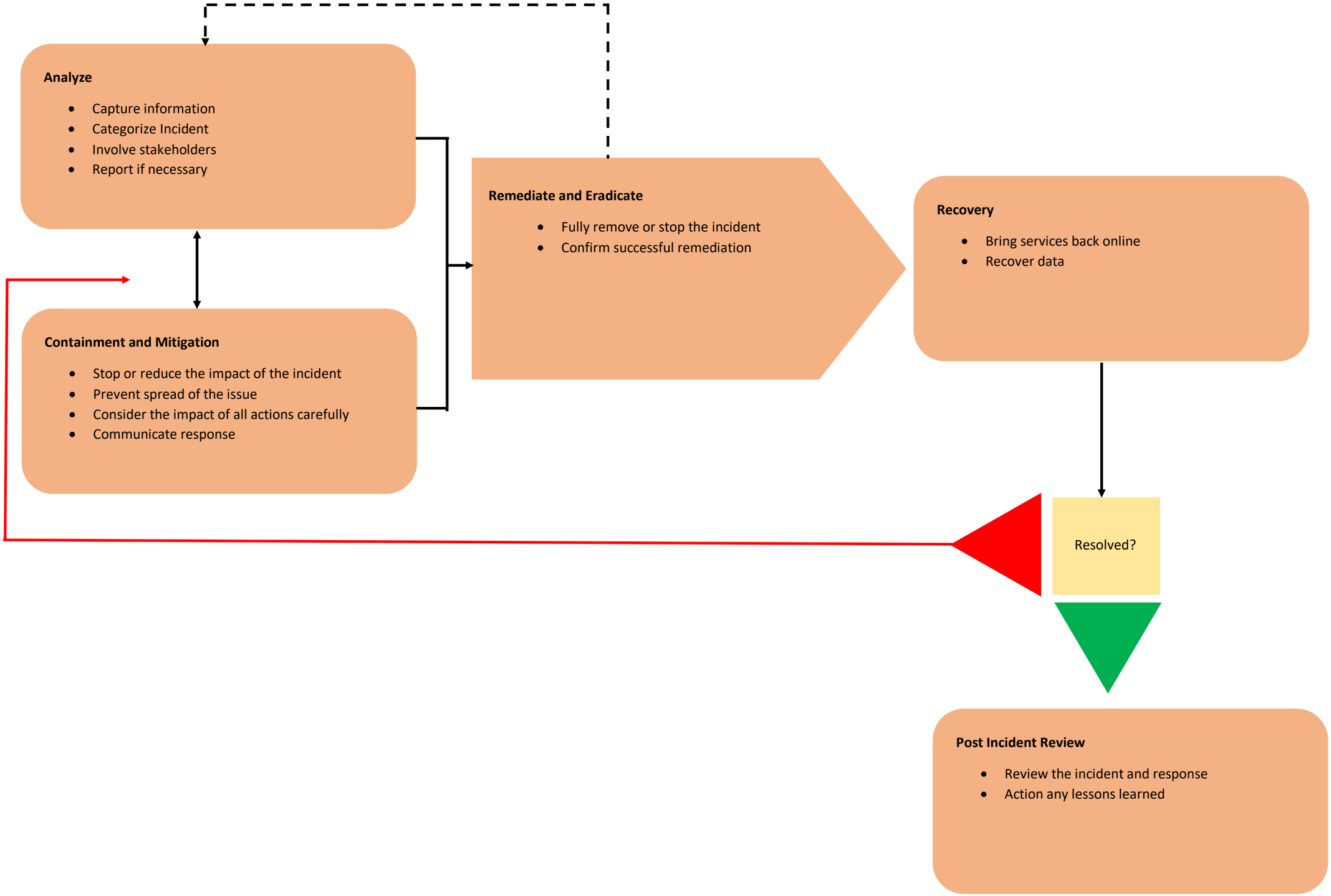
Systems will be returned to their normal state, any lost or damaged data will be restored from backups.

Post Incident Review

Once the incident has been fully recovered it will be reviewed. The purpose of this review is to establish what lessons may be learned from the incident and what improvements can be made. The review should consider:

- Was the incident response effective and successful?
- Were there elements that could have been handled more effectively?
- What information was not available in the response that would have been useful?

Incident Response Process Diagram



Cyber Security Incident Severity Matrix

Severity	Criteria
Critical	• Over 80% of staff and students (or several critical staff/teams) unable to work • Critical systems offline with no known resolution • High risk to / definite breach of sensitive client or personal data • Severe reputational damage - likely to impact business long term
High	• 50% of staff and students unable to work • Risk of breach of personal or sensitive data • Non critical systems affected, or critical systems affected with known (quick) resolution • Potential serious reputational damage
Medium	• 20% of staff and students unable to work • Possible breach of small amounts of non-sensitive data • Low risk to reputation • Small number of non-critical systems affected with known resolutions
Low	• Minimal, if any, impact • One or two non-sensitive / non-critical devices affected • <10% of non-critical users affected temporarily (short term)

Cyber Security Incident Categories

- **Malware:** Infection on the network, including ransomware
- **Denial of Service:** Typically, a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems.
- **Phishing:** Emails attempting to convince someone to trust a link/attachment.
- **Unauthorised Access:** Access to systems, accounts, data by an unauthorised person (internal or external)
- **Insider:** Malicious or accidental action by an employee or student causing a security incident.
- **Data breach:** Lost/stolen devices or documents, unauthorised access or extraction of data from systems (usually linked with some of the above).
- **Targeted attack:** An attack specifically targeted at the Trust or School - usually by a sophisticated attacker (often encompassing several of the above categories).