Inspiring Futures Through Learning

# Cyber Security Policy

November 2021

*At Inspiring Futures through Learning, we are driven by our pursuit of excellence every day. We have high expectations of learning, behaviour and respect for every member of our community. We create independent, articulate thinkers and learners who have confidence in, not only their individual ambitions, but also those of the Academy and The Trust as a whole. We have collaboration at the heart of everything we do and our vision is to nurture exciting, innovative, outstanding Academies who embrace change and provide a world-class education for all it serves.*

***Including all IFtL Schools, Milton Keynes Teaching School Alliance and Two Mile Ash Initial Teaching Training Partnership**

| | | |
|---|---|---|
| **Policy name:** | | Cyber Security Policy |
| **Version:** | | V1 |
| **Date relevant from:** | | November 2021 |
| **Date to be reviewed:** | | November 2023<br>*This policy will be reviewed every two years unless legislation dictates otherwise. Recent changes in Legislation will need to be read and used to review this Policy.* |
| **Role of reviewer:** | | IFtL Head of Operations |
| **Statutory (Y/N):** | | N |
| **Published on website*:** | | 3C |

| | |
|---|---|
| **Policy level**:** | 1 |
| **Relevant to:** | All employees through all IFtL schools and departments |
| **Bodies consulted:** | |
| **Approved by:** | IFtL Board of Trustees |
| **Approval date:** | 25th November 2021 |

**Key:**

**** Publication on website:***

| **IFtL website** | | **School website** | |
|---|---|---|---|
| 1 | Statutory publication | A | Statutory publication |
| 2 | Good practice | B | Good practice |
| 3 | Not required | C | Not required |

***** Policy level:***

1. Trust wide:
   - This one policy is relevant to everyone and consistently applied across all schools and Trust departments with no variations.
     - *Approved by the IFtL Board of Trustees.*
2. Trust core values:
   - This policy defines the values to be incorporated fully in all other policies on this subject across all schools and Trust departments. This policy should therefore from the basis of a localised school / department policy that in addition contains relevant information, procedures and / or processes contextualised to that school / department.
     - *Approved by the IFtL Board of Trustees as a Trust Core Values policy.*
     - *Approved by school / department governance bodies as a relevantly contextualised school / department policy.*

3. School / department policies
   - These are defined independently by schools / departments as appropriate
     - *Approved by school / department governance bodies.*

# Introduction and Context

Over the last few years, schools have become more and more reliant in IT systems and infrastructure to deliver critical services.
At the same time, the threat from criminals and other bad actors has increased exponentially.

As of May 2021, Microsoft monitoring of ransomware attacks revealed that 60% of all detected attacks were aimed at schools and educational establishments.

This policy aims to set minimum standards for schools with the aim of ensuring that their systems are as protected as they can be against the threat of ransomware, malware and cyber-attack.

Some of the language in this document may be technical but we have tried to keep it as understandable as possible.

# Firewalls and Perimeter Protection

Schools must have an appropriately configured firewall between their network and the internet. Most of the time, the router that is supplied by the broadband provider will also contain the firewall. All firewall and gateway devices must have their default username and password changed to something appropriately secure (a hard to guess password with at least 8 characters). The new details should be kept secure and only shared with those that need to know them (IT support staff or contractors).

# In-School Services Accessible from The Internet

As far as possible, schools should attempt to secure access through their firewall or gateway by closing off any unnecessary ports.
Many ports may need to be open in order to facilitate the operation of telephones, software services and other systems but, where possible, a default position of closing ports and only opening those that are necessary, should be adopted.

Schools should keep a secure list of open ports, along with the reason for having them open so that any gaps in security can be closed if software or systems change.

If it is not practical to maintain a default position of keeping ports closed unless required, this must be documented, agreed and signed off by the school SLT/Governing Body/Trustees.

Where schools operate a VPN to allow staff access to the network from outside the school, each user must have their own individual username and password in order to track access. Accounts must not be shared. Multi Factor Authentication must be enabled to all remote access where it is technically possible to do so. Where this is not possible, alternative measures should be investigated to further secure access via VPN.
Admin access should never be allowed via VPN.
All email accounts associated with VPN access must have MFA enabled.

## User Devices

There are many steps to take to ensure that user devices are secure.
Schools should maintain a list of devices along with details of their operating system and who the devices are issued to.

All devices should be set to automatically download updates and users must be instructed to allow updates to run as soon as they are received (or at the end of the day they are received).
Users must also be instructed on the correct way to close down their device at the end of each day. Merely closing the lid does not allow a device to close down and this can prevent important updates from installing.

Schools should have a process in place to ensure that this is checked on a regular basis. Unpatched devices are a security risk to the whole school network. Regular spot checks of devices to ensure updates have been deployed should be considered as part of your IT support package.

All devices must have anti-virus software installed and operational. Windows comes with built-in virus and threat protection. It also has a software firewall which should be enabled.

When purchasing and issuing new devices, ensure that any unnecessary software is removed. Many manufacturers bundle unnecessary software with new devices.
Some devices may also come with a default configuration which includes an admin account already set up. These 'out of the box' account details are often available on the internet and should be removed before issuing devices to staff or pupils.
It may be wise to consider re-imaging all new school devices as standard, to ensure that they all have the same configuration before deployment. This may not be practical in all cases but is the best way to ensure that devices are standardised.

New devices should have a TPM chip included in the configuration. This adds an additional layer of security, and ensures forward compatibility with Windows 11.

## Passwords

Passwords must be secure and you should never use your work account password for any other account or device.
If your password is discovered, or leaked, and you use it on multiple accounts or services, all of those services are at risk.

Passwords should be strong and difficult to guess. Current advice from the National Cyber Security Centre is to use 3 random words as your password.
It is far better to pick a strong password and stick with it than it is to change your password every 3 months.

If necessary, use a password manager. Many web browsers have password management built in, or third-party password management applications are available.

Admin level users must have multi factor authentication enabled. This means that, even if your password is stolen, your account is still safe unless the attacker also has access to your MFA device. You will require assistance from your IT team to implement MFA.
Where possible, all users should have MFA enabled on their email account.

Everyone should check the following to see whether their details have ever been part of a data breach;

- https://haveibeenpwned.com/ - This page will tell you if your email address has ever been breached. Many emails have, so don't panic if you are on the list. If you haven't changed your password since the breach date however, you should do so straight away.
- https://haveibeenpwned.com/Passwords - If your password is in this list, you should change it and never use it again. It may be associated with a data breach that is linked to your email address, or it may be a common password that is used by many people. Either way, if it is in this list, it is unsafe and should be changed straight away.

## Malware Protection

All devices should have auto-run disabled to reduce the risk from malware that arrives via email or from portable devices.

## User Accounts

When creating user accounts, consideration must be given to the level of access required to ensure that it is appropriate to the role.
Users should have hierarchical access rights, allowing them to see the data and settings required for their role, and nothing beyond that.

Admin accounts should never be used as a standard user account. Where users have an admin account, they should also have a general, daily use account and the admin account should only be used when carrying out admin level tasks.
Admin accounts must be secured with multi-factor authentication.

## User Training

The risk from malware, ransomware and other cyber-attack is increasing, and is ever changing. It is critical that all users remain aware and stay up to date on current techniques used by cyber criminals.
The NCSC provides several training resources including a training video which anyone can access for self-directed learning. The resources are also available as a training package for schools to use as a training tool in an inset or twilight session. (This course is now integrated into Smartlog).

All staff are vulnerable to this type of attack, so it is important that all staff are trained and aware of protective measures.

Schools should assign training and keep a record of how training was delivered and who has completed this.

It is vital that training is refreshed regularly, annually as a minimum, to ensure that staff vigilance remains high.

## Response, Back Up and Continuity Planning

All schools must plan for response and recovery from a cyber security incident, including a ransomware attack.
This will involve documenting a planned response as a part of their Business Continuity Plan, or as a stand-alone document.

We do not currently have a template for this as response will vary according to local arrangements at school, whether they have in-house or bought in IT support and what systems they use.
However, some common areas will be;

- Provision of backups and how a planned restore or roll back would happen
- A list of contacts to assist with recovery (MAT contacts, IT support, insurance etc)
- How response is practiced to ensure that it is appropriate

Part of the practice could involve the use of the NCSC's 'exercise in a box' which is a free of charge service available online.

When considering backup and recovery plans, the following must form part of your process;

- Identify your business critical data – Which systems or information can you not operate without? If there was a malware attack, what could you re-build or recover from elsewhere, and what would be a catastrophic loss? Planning and curriculum resources may exist elsewhere, in Teachers' systems for example, but your MIS data, HR data and safeguarding data are highly sensitive and business critical. Are these in systems that are protected effectively? Are they backed up appropriately? Have you tested the recovery process to ensure it works? Just assuming that it should work could be a costly mistake.
- Check your backup systems – Are you backing up the correct data or are you wasting space by backing up ancient folders or irrelevant data? How frequently is recovery tested? This does not have to be full disk recovery, try restoring individual test files or folders. Are your backups offline? i.e. if you have a ransomware attack, is your system just going to replicate the infection to your backup? How many versions do you have if this does happen? Are your backups protecting you adequately?
- Check third party processor systems – Many systems are used in schools including safeguarding systems, parent communication platforms and education systems for pupils to name but a few. How well protected is the data in these systems? Is their data backed up? Are they protected against cybercrime and the loss or theft of data? You should obtain and store details on this from each third-party provider that processes data on your behalf.
- Take a risk-based approach – Evaluate the risk to each of your systems. As an example, SIMS, hosted on a school-based server is a much higher risk than curriculum planning hosted on Office 365 (SharePoint, OneDrive or Teams).

Office 365 has 90-day recovery built in which means that version history is stored for 90 days. Any document can be restored to a previous version that existed in the 90 days prior to any change.
School based servers do not generally have this level of protection and are more vulnerable to attack so their built-in protection needs to be resilient.

In addition to this, some guidance on what to consider during an attack, and how to respond, are covered here.

## Responding to a Cyber Incident

A cyber incident can mean various things. In order to identify the most appropriate response, you need to analyse the incident before taking further action.

If you are reacting to a live incident of a severe nature, for example, if your systems are being encrypted by malware, this first step to take is to isolate your systems by unplugging from the internet and shutting everything down.
This type of event is rare, but if it does happen, you may stop it from being as severe as it could be by disconnecting services.

Ensure that key members of staff are aware of what to do in such an event.

For anything other than events such as those described above, the following is an example response plan. Schools should use this as a template for a site-specific plan based on their own systems.

1. Assess the impact of the event. What has been attacked? How is this impacting you? Can normal operation continue and, if not what do you need in order to deliver education while the event is being mitigated?
2. Categorise the incident. What type of event is it and what needs to be done about it? Who needs to know about it?
3. Escalate, if required, to SLT, the Trust, legal representatives.
4. Plan the response. This should be a team effort following the notifications required in steps 2 and 3 above.
5. Recover. Carry out the plan set out in section 4 above.
6. Report and reflect. Reporting may have started before this point but ensure that this is completed. Reflect on how this event occurred, what has been learnt and what mitigation is required to prevent this from happening again in the future.

This is a very basic plan, and it will need adapting to the circumstances of the incident. Due to the evolving nature of cyber-crime, it is impossible to plan for every incident, so a basic plan that can be adapted to each type of incident can be the best solution.

Ensure that your plan includes key contact details for critical persons including your IT department, senior management, legal team, HR, Insurance and key Trust contacts.

Whatever the incident, there are several critical steps to consider.

- Contain the breach/incident. Try to stop the problem from spreading by containing it as far as possible. If you have VPN access, ensure that no-one remotes in and unwittingly spreads the issue.
- Analyse your data. Document, as far as possible, what you think has been lost or which systems were affected.
- Communicate! Keep stakeholders informed at each step. Appoint an incident manager and ensure that all communication goes through that person.
- Record all actions taken in an incident log, along with the person that has taken the action and the result.
- Consider devising checklists for some typical cyber incidents. Anything that takes the pressure off during an emergency and allows a logical, step-by-step response will be useful.
- Ensure that your cyber response plan is linked into your business continuity plan and your risk register.

## Types of Incident

Cyber incidents can include:

- **Malicious code:** 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) – for example access to someone's emails or account.
- **Insider:** Malicious or accidental action by an employee causing a security incident.
- **Data breach:** Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).
- **Targeted attack:** An attack specifically targeted at the business - usually by a sophisticated attacker (often encompassing several of the above categories).

## Core Response

A brief description of the stages of response are shown here.

### Analyse

This stage of the incident involves everything from technical analysis through to a review of social media reactions.

It is important to ensure tasks are prioritised carefully and findings are constantly reviewed and correlated, as these may lead to new tasks.

Usually, the initial priority is to understand enough to take containment/mitigation actions and ultimately remediate the attack.

**Contain/Mitigate**

Once you're certain it's safe to do so, you should take steps to reduce the impact of the incident and prevent things from getting worse. This usually involves such things as blocking activity, isolating systems and resetting accounts. It may also involve non-technical actions such as media handling.

This stage may require critical decisions such as taking a core business system offline. It is important to consider the consequences of any such actions, *both good and bad*.

You should also evaluate the possibility that the attacker might react to your actions, or bury themselves more deeply in the network (often in the case of targeted attacks). In some cases, it may be better to monitor and analyse further before action is taken. This decision should be taken with your IT support and in consultation with the Trust.

**Remediate/Eradicate**

The aim of this stage is to fully remove the threat from your network and systems. This often involves similar actions to containment but is sometimes coordinated so that all actions are carried out simultaneously.

It is important to confirm that remediation has been successful before to moving to the recover stage - this may involve monitoring for a period. Some analysis may continue in this stage too.

**Recover**

At this point, systems are returned to 'business as usual'. Clean systems and data are put back online and in some cases, final actions are taken to handle regulatory, legal, or PR issues.

**Throughout the response, all tasks and findings should be tracked. Findings and analyses should be correlated, response actions re-prioritised.**

**Post incident review and close down - Learning from the incident**

A post incident review should cover:

**Lessons from the incident itself**

- Are there security improvements which could have prevented the incident, or enabled earlier detection?
- Consider both the tactical fixes that would have prevented or detected this incident as well as strategic solutions that may only be identifiable across multiple incidents. For example, ineffective governance processes leading to multiple intrusions through previously un-recorded, internet-facing, assets.
- In particular, was there any information which would have significantly helped your response but which was difficult or impossible to obtain? *Make a plan to gather this data ahead of any future attacks.*

**Lessons from the response**

- Was the response successful and effective?
- Were there elements which could have been handled better?
- Was there data which could have been useful but wasn't available (For example, the right logs, or something that was overwritten early in the response?). *Keeping a record of activities during the response will assist with this review.*

**Asking questions**

You should consider these issues across people, process and technical capabilities.

For example:

- Were the relevant data and tools available to enable the analysis?
- Did the processes and communications work well?
- Were the right people involved and empowered to make the necessary decisions?