



# Cyber Security & Awareness Policy

**Date Adopted: 28<sup>th</sup> April 2022**

**Reviewed: October 2023**

**Author/owner: Board of Trustees**

**Review: Annually**

**NB.** 'Trustees' means the Directors referred to in the Trust's Articles of Association

## History of most recent policy changes

Version	Date	Page	Change	Origin of Change e.g. TU request, Change in legislation
V1.0	September 2021		New policy introduced for the Tarka Learning Partnership Central Trust Team and Schools within the Trust	Requirement for central policy to set guidance and expectations for protection of the Trust against cyber crime and cyber security.
V1.1	March 2022	Appendix 5	DfE Cyber Recovery Template added and small amendments to meet compliance	DfE template and Risk Protection Arrangement Requirements
V1.2	June 2023	5	Roles & responsibilities added	Best practice
V1.3	September 2023		Minor updates. Addition of password guidance appendix 2	Recommendations from IT Security Audit

## Contents

History of most recent policy changes.....	1
1.0 Introduction.....	4
2.0 Purpose Statement.....	4
3.0 Scope.....	4
4.0 Roles & Responsibilities.....	5
5.0 Common Cybersecurity Threats.....	5
6.0 Users.....	6
7.0 Risk Management.....	7
8.0 Device and Network security.....	8
9.0 Cloud Systems and Software Providers.....	9
10.0 Working remotely.....	10
11.0 User Education & Awareness.....	10
12.0 Monitoring, Preventative Action, Reporting & Incident Management.....	11
12.1 Monitoring.....	11
12.2 Preventative Action.....	11

12.3 Reporting .....	12
12.4 Cyber Response Plan.....	12
13.0 Disciplinary Action .....	13
14.0 Use of Appendices.....	13
Appendix 1 – Change Request Form .....	14
Appendix 2a – Cyber and Information Security Checklist – schools migrated to Trust IT System.....	17
Appendix 2b – Cyber and Information Security Checklist – schools outside @tarkatrust.org.uk domain .....	24
Appendix 3 – Visitor Access to IT systems .....	31
Appendix 4 – Cyber Security Awareness .....	33
Appendix 5 – Model DfE Risk Protection Arrangement Cyber Response Plan .....	34

## 1.0 Introduction

Cyber-crime and cyber security pose a significant risk of data theft, scams and security breaches that can have a detrimental impact on the operations of the Trust. The management of these risks is vital to protect the Trust's resources, prevent financial loss, ensure business continuity and protect its reputation.

Cyber security is about protecting the devices we use and the services we access online from theft or damage and preventing unauthorised access to personal data stored on these devices and in the cloud. This policy should be used in conjunction with the schools e-safety policies, acceptable use policies, data protection and information security policies.

## 2.0 Purpose Statement

The purpose of this policy is to ensure that the risk of harm to the activities of Tarka Learning Partnership through cyber-crime is minimised through:

- A collective understanding of cyber security and how it supports the overall organisational objectives.
- Active Risk Management processes that are appropriate for the organisation.
- Creating a positive cyber security culture through engagement and training.
- Active Asset Management .
- Protecting systems and data through design and keeping them protected through their life cycle.
- Ensuring data is protected from unauthorised access.
- Active monitoring, reporting and incident management.
- Understanding the supply chain and embedding compliance to cyber security within procurement.
- To comply with regulatory obligations.
- To prepare a Cyber Response Plan.

## 3.0 Scope

Tarka Learning Partnership relies on the use of ICT to enhance teaching and learning and conduct its administrative processes. Every member of staff, trainee, pupil, volunteer and visitor may have access to the Trusts IT systems in order to carry out their professional or educational activities.

This policy covers staff currently employed by the Trust, pupils, volunteers, workers and DPSCITT trainees.

The Policy covers all Trust IT systems, local networks, trust-wide networks or cloud software services and all devices used to access these networks and services, including personal devices from any location and when representing Tarka Learning Partnership.

#### 4.0 Roles & Responsibilities

Trustees: Have overall responsibility for managing the risks in relation to cyber security and monitor this through the Strategic Risk Register and reports from external audit and the Trust DPO.

Chief Operations Officer: Is responsible for leading and developing the IT Strategy, to ensure it supports the highest level of protection against cyber threats, receives regular updates on the risks posed by cyber threats and cascades this information and ensures training is part of the program of induction for all staff.

Information Governance Leader: Ensures compliance in the supply chain and has oversight of information security.

Head Teachers: Must ensure all staff are provided with Cyber Security Awareness training upon induction and receive annual updates.

#### 5.0 Common Cybersecurity Threats

The nature and range of issues and threats suggests that all schools are likely to experience some form of cybersecurity incident at some point. These usually enter the system through emails, websites and removable devices.

The Trust does not allow the use of USB or other removable devices unless expressly permitted, therefore the greatest risk to cyber security is from email and access to unsecure websites.

The Trust's IT system uses Microsoft Exchange Online Protection mail filtering service. This service reduces the amount of malicious spam, spoofing and phishing emails that arrive in our inboxes. However, users will still occasionally receive them and should be aware of how to recognise malicious spam, spoofing or phishing emails and delete them or report them immediately without opening them. These emails are likely to contain attachments, embedded links or a request for information that can cause significant harm to the IT systems or make the

Trust vulnerable to fraud.

Spam takes the form of unsolicited emails from companies offering 'discount prices' or 'free software', these should be deleted without opening them.

Spoofing and phishing emails take the form of pretending to be a bone fide company or person. Beware of emails claiming to be a bank or a company attaching an invoice, request for overdue payment or a request for urgent information, these emails may contain spelling mistakes, look unprofessional, they have an unusual email address or just not feel right. Do not open them; report them by forwarding to [report@phishing.gov.uk](mailto:report@phishing.gov.uk) then delete the unopened email, the email should not be forwarded to any other person.

Email addresses are sometimes hijacked to send malicious emails that may contain harmful material. If you receive an email from a colleague or other trusted organisation that appears unusual or suspicious, alert and check with the sender before opening it. If their email has been hijacked they are then able to take action to secure their email account and take action to protect their systems. You should notify this to [IT@tarkatrust.org.uk](mailto:IT@tarkatrust.org.uk) so that colleagues within the Trust can be alerted, as emails are often sent to all contacts within an address book.

If you are in doubt as to the authenticity of an email do not open or click on it. If you do not feel confident to delete it contact the originator via their externally published contact methods to verify the authenticity of it.

The Trust recognises that malicious emails can appear bone fide and that sometimes these emails may be opened in error. Where this happens, it is important that it is immediately reported to a member of the Senior Leadership Team and IT Support by following the procedures laid out in section 11 of this policy. This will enable the school to minimise any risk to its IT systems and protect its data.

Users should exercise vigilance and care when accessing external websites and should ensure the padlock symbol is displayed on the left side of the address bar to indicate the site is secure, also take note of the URL address to ensure it is authentic, if it has spelling mistakes or additional symbols it may be an imposter site. Users should not follow links that pop-up within web-browsers, particularly where they offer incentives such as prizes.

Do not follow links to websites from emails, unless you are confident that the email is authentic. Avoid responding to requests to follow a link to validate credentials unless you are expecting it as part of a process you are following. If in doubt, go through the company's published web address via your internet browser.

In the event a link is followed that turns out not to be genuine or results in information being submitted to an unknown party, please record as many details as possible and report the incident to a member of the senior leadership team in order that the site can be added to the list of blocked sites, the security to the schools systems can be improved and the event checked to ensure they has been no data breach. See section 11 of this policy

## 6.0 Users

Users of the IT system are the first line of defence against cyber threats and the awareness and vigilance of staff when using IT is paramount to the protection of the schools data and IT systems.

The Trusts seeks to establish an open and positive culture in relation to cyber awareness to ensure there are no barriers to incident reporting and information sharing.

We do this through

- Development of policies relating to the safe use of IT, including acceptable use and data protection and information security policies that give guidance on best practice
- Annual staff training and awareness sessions
- Common IT Support for systems throughout the Trust
- Sharing information on new cyber threats as they emerge

We actively encourage all users to report incidence of suspected malicious cyber activity through the appropriate channels as described in section 11 of this policy.

Many security features of the Trust's defence against cyber security work in the background and are unseen by the user, others have a direct impact upon the way in which we work. The Trust aims to strike a balance between effective security controls and the needs of the user. For example, different types of users will have different settings for lock screen after a period of inactivity depending upon their role and the type of data they have access to. Users who have greater access to sensitive data or administrative controls, are more likely to notice more of the cyber security measures in place.

These security controls may sometimes be perceived as an inconvenience but are vital to protect our IT systems from cyber threats or data breaches. Where a user needs support or a review of any of the security measures in place on their account because it prevents them from carrying out their work, they must discuss this with their Head Teacher and IT support. Where a change is agreed this must be submitted on the change request form in appendix 1. Changes may only be implemented where the change does not compromise the overall safety of the Trust's IT system.

Users agree to safe use of IT and accept their responsibilities for managing and reporting cyber security incidents by abiding by and signing the Trusts Acceptable Use of IT Policy.

## 7.0 Risk Management



Cyber Security will be managed as a separate line on the Trusts Risk Register within the Trusts existing Risk Management Policy and Strategy.

Risks will be assessed via the Cyber Security checklist Appendix 2 which will be completed and reviewed annually, when there is a change to the IT system or immediately after an incident.

Responsibility for the completion of the checklist lies with the COO for centrally managed systems and policies and with Head Teachers where implementation is at school level.

## 8.0 Device and Network security

The Trust has designed its IT strategy to ensure all basic security features that protect the Trust's data and keep the IT network safe from cyber threats are enabled. The security features within the strategy have been set to be complex enough to provide robust protection from cyber threats without putting barriers in the way of users that may inadvertently lead to weaker systems being designed by users e.g. password protection.

These security features include :-

- Firewall to protect the Trust's network
- Use of group policies to automatically manage user permissions at the appropriate level for their role
- Using secure settings on devices and software, such as automatic lock screen after a period of inactivity
- Strict controls on user privileges such as the number of staff who have access to administrative passwords to manage the Trusts & schools domain and license accounts
- Automated management of starters and leavers
- Anti-virus software that is regularly updated to protect the system from viruses and malware
- Regular windows updates and software patches
- Cloud service software updates
- Password complexity and 2-factor authentication where available and relevant
- Use of Microsoft Edge password manager
- Sound Asset Management processes
- System inventory and baseline build for devices
- Elimination of the need for use of USB and other external drives
- Agreed processes of managing disposal of devices and hardware
- Azure system back-up and cloud-based file and document storage with recovery testing
- Guest wifi access

The Trust cannot completely eliminate the risks from cyber threats and relies on the vigilance of users to ensure the highest level of protection.

Users of the Trust's IT Systems should

- Avoid posting specific details about the school and their role on social media sites
- Ensure work accounts have different passwords to personal accounts
- Set strong passwords for their work accounts
- Not share their passwords with anyone else
- Not write them down. If a password needs to be written down it should be kept in secure physical storage such as a locked cabinet or safe & in an envelope that has been signed & sealed over all joints.
- Use Microsoft Edge Password Manager to securely store passwords if required for your role – see appendix 2
- Not use work email address to access personal sites/services
- Always lock their screen whenever leaving their device unattended
- Ensure personal devices used to access work accounts have the latest version operating software on them and are protected by anti-virus software.
- Only download software from official stores
- Ask for help if they feel they are being compromised or pressured to provide personal details or information that could compromise the IT systems or the school's data.
- Feel confident to report to a member of the Senior Leadership Team and IT Support if they click on a malicious link
- Be able to discuss IT security measures with a member of the Senior Leadership Team and IT support where it is not possible to follow security advice as it create a barrier to effective working.

Visitors to the Trust/School who require access to the IT systems will sign an acceptable use of IT policy statement when joining the network. Visitors should be informed that removable devices should not be used to access their documents, this can be managed by login to their cloud storage area or by emailing the documents to themselves, or in exceptional circumstances a named contact within the school. The guidance in Appendix 4 can be issued to visitors before their visit.

## 9.0 Cloud Systems and Software Providers

The Trust maintains many relationships with other providers and suppliers where the use of IT exists. The extent of reliance on IT and the level of risk will vary but where the Trust relies on these services for business continuity, such as email servers, MIS, course delivery it should be assured that those providers have adequate measures in place to protect from cyber threats through evidence of their compliance with Cyber Essentials and where the data is of a sensitive nature an accreditation of ISO9001/27001. In the case of key systems containing highly

sensitive data such as MIS, Finance and Safeguarding software, these suppliers should all be approved and available through the government digital market place or National Frameworks. DPIA assessments will be used to gather the key information during the procurement process.

Software as a Service is growing in use across the Trust, particularly systems such as CPOMS, Bromcom, iTrent and Access that host the Trust's most sensitive data. Users should set complex password as per the guidance issued in Appendix 2 of this policy and take additional care to ensure that privacy measures are followed, including locking the screen when leaving the desk or having a visitor arrive at the desk.

Data should not be transferred out of these systems on to any other device media and should only be transferred between schools using the in-built file transfer protocols within the software and via the DfE file transfer system.

Consideration of data protection of IT and systems must take place during the procurement process and is set out within the Procurement Policy and workflow appendices to that policy.

## 10.0 Working remotely

Pupils and staff need to be able to access school systems remotely to extend learning opportunities or support administrative functions. The use of staff devices at home brings with it the risk of unauthorised access to sensitive information. Storing all files and data in the cloud reduces the risk of data loss. Data should never be stored on or transferred to a removable drive or saved on the local drive to reduce the risk of loss of data if the device is lost or stolen.

Staff should ensure good practice when working remotely and should always use their work device. Staff should not allow others outside of the organisation to use their work device and the device settings must always require the user to enter the password and should not be automatically remembered by the device.

Work accounts or devices should never be connected via an unsecured network. Staff may use their own mobile phone to access work accounts, the device should be password protected with at least 6-characters or bio-metric identification and have anti-virus software enabled. This personal device must not be a shared device.

## 11.0 User Education & Awareness

Educating and training is essential so that all users understand their cybersecurity obligations and responsibilities.

This will take the form of training at different levels within the organisation.

- IT Support and local network managers will keep abreast of cyber security updates and technical training as part of their on-going work
- Trust Senior Management will undertake termly cyber security training updates from NCSC or other appropriate sources, meet with IT Support and cascade new information to staff
- All staff will receive Cyber Security Awareness training supported through this policy

Where all users actively manage and report cyber activity, we all contribute to the continuous improvement of internet safety to ensure continuity of education for our pupils.

## 12.0 Monitoring, Preventative Action, Reporting & Incident Management

The Trust operates a positive cyber security culture and all users, whether staff or pupils, should feel secure in the knowledge that being open when things go wrong will not result in sanctions, but the information will be used to improve the network's security. Preventative action and early reporting of an incident helps the Trust identify risks and minimise any potential damage to its systems and may prevent loss of data that could lead to a serious data breach.

Through the vigilance of users and established good practice the majority of malicious threats will have been dealt with without the need to implement an incident management plan.

### 12.1 Monitoring

The Trust's IT systems monitor user activity. The internet filtering system detects attempts to access websites or materials considered to present a risk of harm and can detect where multiple attempts have been made to access a user account. The Trust may share IT monitoring reports with external services to help identify inappropriate use or safeguarding issues or investigate incidence of cyber-crime activity.

### 12.2 Preventative Action

These are the actions users must take if they suspect they have received malicious IT Communications -see section 4 of this policy for more detail

- Spam email – delete without opening the email.
- Spoofing and phishing emails - do not open, report them by forwarding to [report@phishing.gov.uk](mailto:report@phishing.gov.uk) then delete without forwarding to others Hijacked email from a Trusted source - alert the email owner and notify [IT@tarkatrust.org.uk](mailto:IT@tarkatrust.org.uk) and delete the email

### 12.3 Reporting

The Trust recognises that from time to time a user may inadvertently open an email or click on an embedded link that may have created an opportunity for malicious software to enter the IT system that could immediately or eventually lead to loss of data or functionality of IT.

In this event the user must

- Act immediately to isolate the device from the network by removing the LAN connection or disconnecting the wifi (if the user has this ability). You should **NOT** turn off the power supply to the device as this may hamper ability to retrieve data.
- Note as much information as possible
- Immediately report the incident to IT Support and a member of the schools Senior Leadership Team, providing them with their user account details.
- Wait for approval before reconnecting the device to the network or logging back into the user account from any device
- Assist with any follow-up investigation into the incident
- Implement any recommended measures that will improve future security

### 12.4 Cyber Response Plan

The incident will be managed by a member of the senior leadership team with IT Support. Once an event is recognised as a genuine Cyber attack the processes laid out the schools Cyber Response Plan will be followed. The procedures followed to manage the incident will vary depending upon the severity of risk posed by the incident.

Incidents dealt with in accordance with the procedures laid out in the school's Cyber Response Plan may involve notification to third parties such as the schools' insurers, the Information Commissioners Office or the Police.

Incidences must be dealt with sympathetically and the identity of the user kept confidential where possible and used only for the purposes of investigating the incident. Users will not be named in communications with other staff unless it is strictly necessary to do so.

The first action to take in all reported incidence is to ensure the safety of the network and remove the device from the network if this has not already been actioned by the user. Where an incident appears to pose a significant risk to either loss of data or functionality, a member of the Senior Leadership Team and or IT Support may take the decision to temporarily suspend the use of all devices and network services whilst initial investigations are carried out. In all cases the amount of downtime will be kept to the minimum required to ensure the safety of the network.

In the case of a ransomware attack, the Trust/school must **not** pay any money to any parties in exchange for access to its systems or the retrieval of data. The police must be notified of any such demands.

Where the incident involves data theft or a compromise of personal data, the GDPR lead for the Trust must be informed and processes as laid out under the regulations for managing data breaches followed. Incidence incurring a financial cost, such as making a payment following receipt of a bogus invoice should be reported to the police at Action Fraud and also reported to the Chief Finance Officer of the Trust.

After the incident has been dealt with, there should be a review of what happened, how and what (if anything) was damaged so that lessons can be learned. In the process of further investigation, the investigators should maintain objectivity and try to get a complete picture of usual practice by gathering the perspectives of other similar users of the system whilst maintaining confidentiality. The investigation should focus on the facts available at the point at which each decision was made and not on the final consequence of the chain of those decisions.

The outcome of an investigation may lead to changes to device & system configuration, software updates, process changes or further training. These changes should be fed-back to the user reporting the incident and communicated to all users via suitable communication systems.

### 13.0 Disciplinary Action

The Trust does not seek to discipline staff for reporting incidence of cyber security risk and an open and proactive approach to the management of cyber security is required by all users to reduce the risk of harm from cyber-crime, all reported incidents will be reviewed fairly and findings used as development opportunities for all staff to reduce the risk of a reoccurrence.

However, that does not mean that users are not accountable for their actions and disciplinary action will be considered where there was an intent by the user to cause harm or wilful neglect of this policy which prevents action being taken to reduce damage to systems following a cyber incident.

### 14.0 Use of Appendices

The appendices supplied with this policy are template documents designed to supplement each schools suite of IT documentation. All appendices are available as separate word documents. Appendices 3a/b, 4, 5 and 6 must be tailored to the context of each school.

### Appendix 1 – Change Request Form

This form can be made available as a separate electronic document and used to support a change request via the IT Support help-desk function.

IT Change Request Form			
Name of School			
Name of person submitting request		Job Role	
Detail of the request			

Reason for need			
Is this change applicable for other similar users?			
Date change required by			
Approver sign-off			
Approver Name		Date	

## Appendix 2 – Password Policy and Password Management Guidance


*This guidance pertains to schools who have migrated to the @tarka domain. If you have not yet migrated to MS365 ensure you follow best practice for password management as described below within your google domain.*

Secure passwords and password management is an essential component of our cyber security policy. We recognise that in today’s society both in the workplace and home environment there is a proliferation of password use and ever-increasing demands on password complexity which places unrealistic demands on users. This can lead to users devising their own mechanisms to cope with ‘password overload’ such as re-using / adapting the same password & writing down passwords. Attackers exploit these strategies leaving staff and the organisation vulnerable.


To ensure good password management and relieve staff of the pressure of having to remember too many passwords we recommend using Microsoft Edge Password Manager. This is available to all users once you have logged into your MS365 environment. This means that for work purposes you need only remember the password to log into your MS365 account. As 2-factor authentication is also required when you log into your MS365 account for the first time from a new device or periodically as requested, your MS365 account has a double layer of security which will add protection to the password management solution:

### Password Policy:

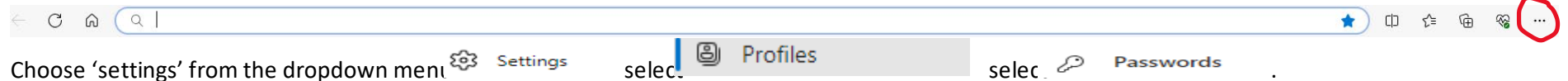


- Staff will be required to set passwords to their MS365 account that contain a level of complexity with a minimum of 6 characters. Staff will be required to change the password every 6 months will not be able reuse the password until the 7<sup>th</sup> change. We suggest using 3 random words principles to set this password as it is more likely to be memorable. MS365 accounts will all require 2FA when logging in for the first time from a new device.
- Staff must ensure work accounts have different passwords to personal accounts.
- Staff must avoid using the same password (or subtle variations of the password) across multiple accounts and should set strong passwords for all work-related accounts using generated strong passwords within Microsoft Edge – please see guidance below
- Staff must not share passwords with anyone else.
- Staff should not write down passwords. If a password needs to be written down, it should be kept in secure physical storage such as a locked cabinet or safe & in an envelope that has been signed & sealed over all joints.
- Staff should not use their work email address to access personal sites/services
- Staff should use Microsoft Edge Password Manager to securely store passwords if required for your role – see guidance below.
- Staff must lock their screen whenever leaving their device unattended – [simultaneously pre Windows logo key  + L ]
- Staff must always inform IT support immediately if they suspect their password may have been compromised.
- Staff may elect to change their MS365 password at any time once logged in by clicking on their login profile (top right of screen) & selecting Password from the dropdown menu.

### Password Manager in Microsoft Edge:

Ensure you are using the 'Work' browser version of Edge 

Click 3-dot crumb at end of search bar



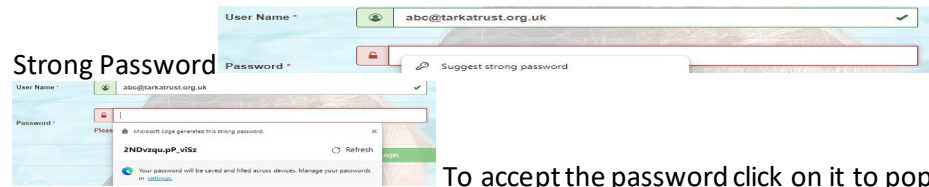
This will allow you to see and manage your stored passwords. To view a stored password, you will be required to enter your MS365 password in a pop up dialogue box.

### Using Password Manager:

To get the most from using password manager save the site login page to your browser 'Favourites' and give it a name that you will easily identify. Most sites will usually remember your username although some sites do not allow that feature.

### Setting a Password:

To set a strong password using the password manager, once you have entered your user-name right click in the password dialogue box and click Suggest



**Strong Password**

It will then display the strong password that has been generated

To accept the password click on it to populate the password field. The password will now be remembered the next time you log back into that site using with the same username.

**Appendix 3a – Cyber and Information Security Checklist – schools migrated to Trust IT System**

Area	Response	Controls/built in features/ supporting policies in place	School Controls & Action taken	Further action required	Who
<i>Training &amp; Staff awareness</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Have all staff received training on general cyber security?		Tarka Cyber Security Policy & training guidance			
Have all staff received training to help them identify phishing/spoofing emails?		Tarka Cyber Security Policy & training guidance			
Are all staff aware of the procedure for reporting incidences of suspected cyber security breaches?		Tarka Cyber Security Policy			

Are all staff aware that they must not connect to their work account through unsecure or public Wi-Fi networks?		Tarka Cyber Security Policy & training guidance Staff Acceptable Use Policy			
Are staff aware they should only login to devices that are protected by suitable anti-virus software if not using a work device		Tarka Cyber Security Policy & training guidance			
Are all staff aware that they should have a minimum of 6-character login or biometric device login if accessing work accounts from their smart phone?		Information Security Policy, Cyber Security Policy & Training guidance			
Are staff aware of the need to keep individuals email addresses private through use of Bcc and exercise care when using the auto-complete function?		Information Security Policy			
Are all staff aware that they should use the built-in systems in CPoms, Bromcom or Egress email for transfer of sensitive data		Tarka Cyber Security Policy & training guidance			
<i>Organisation domain ownership and set-up</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Is your System IT Domain owned by the school/Trust?	Yes	@tarkatrust.org.uk purchased by Trust 2018. School migrating into the system are held as sub-domains and are covered by this ownership		None	
Is the System IT Domain hosted with a reputable registrar?	Yes	Krystal		None	
Is anti-virus installed or Windows Defender enabled on the server(s)	Yes	Windows Defender end point protection		None	
Is Anti-Virus protection installed / enabled on every device	Yes	Windows Defender		None	

Does security protection include enterprise level scanning & remediation?	Yes	Windows Defender		None	
Are all Operating Systems supported and have windows security updated and patches applied at the earliest opportunity?	Yes	Windows auto update window built into system.		None	
Is the management of the network and systems appropriately documented?	Yes	IT Management information held by Ap.Rox Ltd		None	
Are all Central systems properly secured, in particular servers, switches and routers, in secure rooms or cabinets?	Yes	Dedicated server room within the Trust server hubs and RCPA		None	
Are all local systems properly secured, in particular servers, switches and routers, in secure rooms or cabinets?					
Are the tools within the Microsoft Security Centre configured to ensure maximum protection of systems in line with user needs	Yes	Through central IT group policies to manage users			
If you use Google, are the Security Centre features enabled to ensure maximum protection of systems in line with user needs					
Are all devices encrypted	Yes	Bit locker encryption enabled on all devices			
Can threats be intercepted at server & workstation level?		User Account Control is enabled. Firewall enabled. Windows Defender endpoint protection enabled. Microsoft Exchange on line security features enabled		None	
Is your operating system backed up and a copy held off-site?	Yes	Microsoft Azure cloud. Secure and off-site		None	

When was the last test restore of the operating system carried out?	Yes	Tested by XMA Sept '21		Cyclical testing	Ap.rox
Are your files and folders backed up and a copy held off-site?	Yes	MS365 cloud environment	<i>State if files also held elsewhere</i>		
Has the school achieved Cyber Essentials Certification?	Yes	The Trust has accreditation – Autumn '21		None	
<i>Firewalls &amp; Filters</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Is there a core firewall installed and managed?	Yes	Core firewall through ISP		Update information following Broadband procurement	MC
Is there a local firewall installed?	Yes	Yes – switched on by default during system setup		None	
Has the network been penetration tested & if so have any recommendations been acted upon?	Yes			Undertaken by Broadband Provider – update after procurement	MC
Is the network monitored for unusual activity and does it generate activity logs?	Yes			Update details following BB procurement	MC
Are search activity logs monitored ?	Yes	Monitoring through Meraki and filtering software provided by ISP		Update with ISP details	MC
Are you registered with Police CyberAlerts and have the software installed on your school server?					
Can your network manage guest users?			Schools state if this is implemented in your setting		
Is your Internet protected by an industry recognised filtering system?	Yes	Part of Broadband provision		Update with details following procurement	MC
<i>Email security</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Do you use indicators of compromise to check if your email has been accessed?				Microsoft Edge – will inform if accounts have been accessed if it is used	

				to store account details. www.haveibeenpwnd.com	
Do you use encrypted emails.	Yes	MS365 is an encrypted email service.		None	
Do you use encrypted email where sensitive data is being transferred to a 3 <sup>rd</sup> party?		<i>This is the use of Egress or similar + secure transfer of files using built-in tools in Bromcom &amp; CPoms</i>			
Do you have email filtering?	Yes	Use of built into Microsoft Exchange		None	
Does email auto-delete after a period of time?				For TLP Being reviewed – suggest 2 years retention	
Where emails are archived, is this data held securely within the Schools IT systems and document library?					
<i>User Set-up and device management</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Are staff passwords complex and have forced periodic changes?	Yes	Password require a degree of complexity, change at 90 or 180 days depending on staff level & password history of 6 & 12.		None	
Is 2-factor authentication enabled for all staff	Yes	2FA for device login enabled		None	
Is auto screen lock enabled for staff?	Yes	For most users 5 minutes, for class teachers 20 minutes.		None	
Are administrative privileges for domain & IT Administrative User Accounts regularly reviewed and access restricted to key persons only	Yes	Admin rights to domain accounts and main Microsoft accounts restricted to 2 persons, reviewed annually		None	
Have you carefully reviewed access privileges to your document library?	Yes	Active management of permissions and controls through the TEAMS built environment		None	
Are users removed from the IT system immediately upon leaving the organisation	Yes	Managed through Locker Connect, linked with MIS system		None	

If staff use their phones to access work information, is there clear guidance on the level of password protection required to unlock the device	Yes	Information Security Policy - Enablement of biometric recognition or 6-digit security protection		None	
Are all USB sticks encrypted?	NA	The system is set up to allow anywhere cloud access. USB sticks are not used. If needed by exception, then explicit permissions are required & encryption of the removable device			
Can all networked devices be remotely disabled?	Yes	Through central management console			
Is there an inventory of IT Devices which is reviewed annually?	Yes	Assets are fully managed within the Parago software		Give details if there is further work to complete this at your school	
Do you know which school devices are in the possession of staff?		<i>Give details of system used i.e set up in Parago against individual staff or other loans log</i>			
<i>Website</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Is your website domain owned by the school?					
Is the website domain hosted with a reputable registrar?					
Is your website hosted on a secure platform?					
Is web server software fully up-to-date?					
Is your website data backed-up?					
Is there an off-site copy held?					
<i>Policy and Strategy &amp; Support</i>					
Have all staff signed the Acceptable Use declaration?		Staff Acceptable Use Policy			

Are all pupils aware of IT & Email Acceptable use – appropriate to their age?			Please give details		
Do you have a written strategy and renewal plan for IT in place for your school					
Is IT security regularly reviewed with IT Support?	Yes	Yes – minimum of half termly meetings to review Trust IT Policy & Security		None	
Is there a named individual for IT support in school	Yes	Ap.Rox Ltd access via Parago helpdesk		None	
Is digital data destruction managed & a policy in place?	Yes	Trusts IT Strategy document deals with processes for off-boarding of hardware		None	
Is IT security reviewed by Trustees?	Yes	Part of termly part of termly risk management processes		None	
Is there a policy on BYOD/home working	Yes	Acceptable use of IT and Cyber Security Policy		None	
Are there clear expectations regarding usage of Social Media		Trusts use of Social Media Policy	Date relayed to staff		
Has the Trusts Information Security Policy been shared with all staff?		Give details			
Do staff receive training on IT Security and Information Governance as part of their induction?		Give details			
Is there a clear disaster recovery plan that details key IT service providers and their contact details?					
<i>Other Software and Apps</i>					
Does the school follow processes for Data Privacy Impact Assessments	Yes	Schools follow guidance on GDPR toolkit for new suppliers which is written into Procurement Policy			
Have you reviewed all software and applications used in school?		Give details			



Are user permissions for software hosting sensitive data (Bromcom, CPoms, Access) managed by role and reviewed regularly					
Does each user have their own log in access to these accounts?					
Are there systems to prevent former staff from accessing these cloud-hosted systems?					
Is installation of new software applications managed by IT Support?		Give details			
Information Security and /GDPR Compliance					
Are there systems in place for effective breach management?	Yes	Trust centralised system for reporting and monitoring			

**Appendix 3b – Cyber and Information Security Checklist – schools outside @tarkatrust.org.uk domain**

Area	Response	Controls/built in features/ supporting policies in place	School Controls & Action taken	Further action required	Who
<i>Training &amp; Staff awareness</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Have all staff received training on general cyber security?					
Have all staff receive training to help them identify phishing/spoofing emails?					

Are all staff aware of the procedure for reporting incidences of suspected cyber security breaches?					
Are all staff aware that they must not connect to their work account through unsecure or public Wi-Fi networks?					
Are staff aware they should only login to devices that are protected by suitable anti-virus software if not using a work device					
Are all staff aware that they should have a minimum of 6-character login or biometric device login if accessing work accounts from their smart phone?					
Are staff aware of the need to keep individuals email addresses private through use of Bcc and exercise care when using the auto-complete function?					
Are all staff aware that they should use the built-in systems in CPoms, Bromcom or Egress email for transfer of sensitive data					
<i>Organisation domain ownership and set-up</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Is your System IT Domain owned by the school/Trust?					
Is the System IT Domain hosted with a reputable registrar?					
Is anti-virus installed or Windows Defender enabled on the server(s)					
Is Anti-Virus protection installed / enabled on every device					

Does security protection include enterprise level scanning & remediation?					
Are all Operating Systems supported and have windows security updated and patches applied at the earliest opportunity?					
Is the management of the network and systems appropriately documented?					
Are all Central systems properly secured, in particular servers, switches and routers, in secure rooms or cabinets?					
Are all local systems properly secured, in particular servers, switches and routers, in secure rooms or cabinets?					
Are the tools within the Microsoft Security Centre configured to ensure maximum protection of systems in line with user needs					
If you use Google, are the Security Centre features enabled to ensure maximum protection of systems in line with user needs					
Are all devices encrypted					
Can threats be intercepted at server & workstation level?					
Is your operating system backed up and a copy held off-site?					
When was the last test restore of the operating system carried out?					
Are your files and folders backed up and a copy held off-site?					

Has the school achieved Cyber Essentials Certification?					
<i>Firewalls &amp; Filters</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Is there a core firewall installed and managed?					
Is there a local firewall installed?					
Has the network been penetration tested & if so have any recommendations been acted upon?					
Is the network monitored for unusual activity and does it generate activity logs?					
Are search activity logs monitored ?					
Can your network manage guest users?					
Is your Internet protected by an industry recognised filtering system?					
<i>Email security</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Do you use indicators of compromise to check if your email has been accessed?					
Do you use encrypted emails.					
Do you use encrypted email where sensitive data is being transferred to a 3 <sup>rd</sup> party?					
Do you have email filtering?					
Does email auto-delete after a period of time?					
Where emails are archived, is this data held securely within the Schools IT systems and document library?					

<i>User Set-up and device management</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Are staff passwords complex and have forced periodic changes?					
Is 2-factor authentication enabled for all staff					
Is auto screen lock enabled for staff?					
Are administrative privileges for domain & IT Administrative User Accounts regularly reviewed and access restricted to key persons only					
Have you carefully reviewed access privileges to your document library?					
Are users removed from the IT system immediately upon leaving the organisation					
If staff use their phones to access work information, is there clear guidance on the level of password protection required to unlock the device					
Are all USB sticks encrypted?					
Can all networked devices be remotely disabled?					
Is there an inventory of IT Devices which is reviewed annually?					
Do you know which school devices are in the possession of staff?					
<i>Website</i>	<i>Yes/No</i>	<i>Description of features in place</i>	<i>Date action took place &amp; further relevant detail</i>	<i>Record detail and timing</i>	<i>individual</i>
Is your website domain owned by the school?					
Is the website domain hosted with a reputable registrar?					
Is your website hosted on a secure platform?					

Is web server software fully up-to-date?					
Is your website data backed-up?					
Is there an off-site copy held?					
<i>Policy and Strategy &amp; Support</i>					
Have all staff signed the Acceptable Use declaration?					
Are all pupils aware of IT & Email Acceptable use – appropriate to their age?					
Do you have a written strategy and renewal plan for IT in place for your school					
Is IT security regularly reviewed with IT Support?					
Is there a named individual for IT support in school					
Is digital data destruction managed & a policy in place?					
Is IT security reviewed by Trustees?					
Is there a policy on BYOD/home working					
Are there clear expectations regarding usage of Social Media					
Has the Trusts Information Security Policy been shared with all staff?					
Do staff receive training on IT Security and Information Governance as part of their induction?					
Is there a clear disaster recovery plan that details key IT service providers and their contact details?					
<i>Other Software and Apps</i>					

Does the school follow processes for Data Privacy Impact Assessments	Yes	Schools follow guidance on GDPR toolkit for new suppliers. Written into Procurement Policy			
Have you reviewed all software and applications used in school?					
Are user permissions for software hosting sensitive data (Bromcom, CPoms, Access) managed by role and reviewed regularly					
Does each user have their own log in access to these accounts?					
Are there systems to prevent former staff from accessing these cloud-hosted systems?					
Is installation of new software applications managed by IT Support?					
Information Security and /GDPR Compliance					
Are there systems in place for effective breach management?	Yes	Trust centralised system for reporting and monitoring			

## Appendix 4 – Visitor Access to IT systems

We look forward to welcoming you to our school. This document aims to support your visit in relation to using IT from your device whilst in school.

If you require the school to supply a device for you to use during your visit, then please let us know in advance.

The school strongly discourages the use of USB sticks or other removeable device storage media. Instead we encourage you to access your documents via your usual cloud storage or, if you do not store documents in the cloud, email them to yourself to access during your visit.

Guest Wi-Fi is available to all visitors, the password will be made available when you arrive on site. Upon login to the guest wi-fi you will be asked to accept our terms for Acceptable Use of IT as per the follow statement.

By continuing to the internet you are confirming that you have read, understood and agree to the terms of use below

Any individual connected to the Guest Wireless Network, in order to use it directly or to connect to any other network(s), must comply with this policy, the Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

The [school] makes no representations or warranties concerning the availability or security of the guest wireless network, and all use is provided on an as-is basis. By connecting to the Guest Wireless Network, you are agreeing that your device is free from viruses/malicious software and have an up-to-date and appropriate anti-virus solution installed.

The [school], its employees, agents, vendors and licensors takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised or damages arising either directly or indirectly while connected to the Guest Wireless Network.

The [school] reserves the right to disconnect any user at any time and for any reason. The Guest Wireless Network is provided as a courtesy to allow our guests access to the internet. Users will not be given access to The [school] internal network or permission to install any software on our computers.



Inappropriate use of the Guest Wireless Network is not permitted. This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that The [school] may at any time use to make a determination that a particular use is inappropriate:

- Users must respect the privacy and intellectual property rights of others.
- Users must respect the integrity of our network and any other public or private computing and network systems.
- Users must not use of the Guest Wireless Network for malicious, fraudulent, or misrepresentative purposes. ~~is prohibited.~~
- The Guest Wireless Network may not be used in a manner that precludes or hampers other users access to the Guest Wireless Network or other any other networks.
- Nothing may be installed or used that modifies, disrupts, or interferes in any way with service for any user, host, or network.
- Users must not try to upload, download or access any materials which are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. Nor try to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
- Users will not attempt to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

If whilst you are using the Guest Wireless Network you have any concerns regarding the Acceptable Use policy or if you are experiencing any difficulty whilst using the Guest Wireless Network then contact the ICT support team on either [school email], [school phone number or located in the [schools office].

If you have any queries regarding the use of IT prior to your visit, please do not hesitate to contact us.

## Appendix 5 – Cyber Security Awareness

## BE CYBER AWARE – HELP KEEP OUR IT SYSTEMS SAFE.

### Be alert for unsolicited or malicious emails

**Unsolicited Spam**  
emails– do **not** open  
them, just **delete**

**Hijacked email from a  
trusted source** – Check  
with the sender to alert  
them their email has  
been hijacked. If it is not  
genuine do **not** open,  
**forward** to  
[IT@tarkatrust.org.uk](mailto:IT@tarkatrust.org.uk)  
confirming you have  
contacted the originator

**Phishing or Spoof** emails  
– do not open. Forward  
to  
[report@phishing.gov.uk](mailto:report@phishing.gov.uk)  
Then **delete** the email

Do not follow links from  
websites or emails unless  
you are confident they  
are genuine.  
If in doubt go through  
your normal web-  
browser process to login  
into the site .

### What do I do if I click on a link by mistake?

If you suspect you have opened a malicious email that may have created the opportunity for malicious software to enter the IT system. You should

- Act immediately to take the device off the network by removing LAN or disconnecting Wifi if you can
- Note as much information as possible and
- Report the incident to a member of the SLT and IT Support
- Await approval before reconnecting the device to the network or logging in to your user account

If the security measures in place prevent you from doing your job effectively, please raise the issue with a member of SLT / IT Support so that possible solutions can be openly discussed.

This can be printed to pin on noticeboards near workstations.

---

# Risk Protection Arrangement Cyber Response Plan

[Insert School Name]

[Version]

This plan should be used on conjunction with the Trust's Cyber Security Policy

---

<b>Last Reviewed</b>	
<b>Reviewed By</b>	
<b>Next Review Date</b>	

# Contents

- 1. Introduction .....3
- 2. Aims of a Cyber Response Plan .....3
- 3. Risk Protection Arrangement Cover.....4
- 4. Preparation and Additional Resources .....6
- 5. Actions in the event of an incident .....8
- 6. Cyber Recovery Plan.....9
- Appendix A: Incident Impact Assessment.....17
- Appendix B: Communication Templates.....18
- Appendix C: Incident Recovery Event Recording Form .....23
- Appendix D: Post Incident Evaluation.....24

## 1. Introduction

A Cyber Response Plan should be considered as part of an overall continuity plan that schools need to ensure they maintain a minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard.

If a school fails to plan effectively then recovery can be severely impacted, causing additional loss of data, time, and ultimately, reputation.

Incidents may occur during the school day or out of hours. The Cyber Response Plan should be tested, with input from key stakeholders, to ensure that in an emergency there is a clear strategy, which has fail-safes when key personnel are unavailable.

The plan should cover all essential and critical IT infrastructure, systems, and networks. The plan will ensure that communications can be quickly established whilst activating cyber recovery. It is also important that the plan is well communicated and readily available.

The document is to ensure that in the event of a cyber attack, school staff will have a clear understanding of who should be contacted, and the actions necessary to minimise disruption.

### Aims of a Cyber Response Plan

When developing a Cyber Response Plan, you will need to consider who will be involved in the Cyber Recovery Team, the key roles and responsibilities of staff, what data assets are critical and how long you would be able to function without each one, establish plans for internal and external communications and have thought about how you would access registers and staff and pupil contact details. This will allow the school:

- To ensure immediate and appropriate action is taken in the event of an IT incident.
- To enable prompt internal reporting and recording of incidents.
- To have immediate access to all relevant contact details (including backup services and IT technical support staff).
- To maintain the welfare of pupils and staff.
- To minimise disruption to the functioning of the school.
- To ensure that the school responds in a consistent and effective manner in order to reduce confusion and reactivity.
- To restore functionality as soon as possible to the areas which are affected and maintain normality in areas of the school which are unaffected.

**This template is for you to use to help put a Cyber Response Plan in place.**

## Risk Protection Arrangement Cover

From April 2022, the [Risk Protection Arrangement](#) (RPA) will include cover for Cyber Incidents, which is defined in the RPA Membership Rules as:

**“Any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data.”**

Your RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident, you must contact the [RPA Emergency Assistance](#).

To be eligible for RPA Cyber cover, there are 4 conditions that members must meet:

1. Have offline backups. [Help and guidance on backing up](#) is available from the National Cyber Security Centre (NCSC) and should ideally follow the 3-2-1 rule explained in the NCSC blog [Offline backups in an online world - NCSC.GOV.UK](#)

It is vital that all education providers take the necessary steps to protect their networks from cyber-attacks and have the ability to restore systems and recover data from backups. Education providers should ask their IT teams or external IT providers to ensure the following:

- a) Backing up the right data. Ensuring the right data is backed up is paramount. See [Critical Activities](#) for a suggested list of data to include.
- b) Backups are held fully offline and not connected to systems or in cold storage, ideally following the 3-2-1 rule explained in the NCSC blog [Offline backups in an online world](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world): <https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world>
- c) Backups are tested appropriately, not only should backups be done regularly but need to be tested to ensure that services can be restored, and data recovered from backups.

Further Help and guidance on backing up can be found at: Step 1 - Backing up your data - NCSC.GOV.UK. <https://www.ncsc.gov.uk/collection/small-business-guide/Backing-up-your-data>

2. ~~All Employees or Governors~~ who have access to the Member's information technology system must undertake [NCSC Cyber Security Training](#) by the 31 May 2022 or the start of the Membership Year, whichever is later. Upon completion, a certificate can be downloaded by each person. In the event of a claim the Member will be required to provide this evidence.
3. Register with [Police CyberAlarm](#). Registering will connect Members with their local police cyber protect team and in the majority of cases, a cyber-alarm software tool can

be installed for free to monitor cyber activity. Where installed the tool will record traffic on the network without risk to personal data. When registering, use the code “RPA Member” in the Signup code box.

4. Have a Cyber Response Plan in place. This template is for you to use to draft a school-specific plan if you do not already have one. It can be downloaded from the [RPA members portal](#).

For full terms and conditions of Cyber cover, please refer to the relevant [Membership Rules](#) on gov.uk.



## Preparation and Additional Resources

### Preventative Strategies

It is vital education providers regularly review their existing defences and take the necessary steps to protect their networks. In addition to the 4 conditions of cover detailed above, there are several suggested measures that schools can implement to help themselves to improve their IT security and mitigate the risk of a cyber-attack:

- Regularly review IT Security Policy and Data Protection Policy.
- Assess the school's current security measures against [Cyber Essentials](#) requirements, such as firewall rules, malware protection, and role based user access. Cyber Essentials is a government-backed baseline standard, which we would encourage all RPA members to strive towards achieving wherever possible.
- Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.
- Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis. Vulnerabilities within Microsoft Exchange Servers have been the root cause of many cyber-attacks in the last six months. It is highly recommended that on-premises exchange servers are reviewed and patched/updated as a high priority and moving to an Office 365 environment with MFA if possible.
- Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are:
  - If external RDP connections are used, MFA should be used
  - Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect
  - Enable an account lockout policy for failed attempts
  - The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended
- Review NCSC advice regarding measures for IT teams to implement: [Mitigating malware and ransomware attacks - NCSC.GOV.UK](#)
- Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.

### Advice and guidance

The NCSC website has an extensive range of practical resources to help improve [Cyber Security for Schools - NCSC.GOV.UK](#)

## Acceptable Use

Ensure all users have read the relevant policies and signed IT acceptable use and loan agreements for school devices.

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

## Communicating the Plan

Communicate the Cyber Recovery Plan to all those who are likely to be affected and be sure to inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.

## Testing and Review

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

Train key staff members to feel confident following and implementing the plan. Review the plan regularly to ensure contact details are up-to-date and new systems have been included. NCSC have resources to test your incident response with an [Exercise in a Box - NCSC.GOV.UK](https://www.ncsc.gov.uk/section-8)

## Making Templates Readily Available

It is recommended that templates are available to cover reporting, recording, logging incidents and actions, and communicating to stakeholders.

## Actions in the event of an incident

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

- Enact your [Cyber Recovery Plan](#)
- Contact the 24/7/365 RPA Cyber Emergency Assistance:
  - By telephone: **0800 368 6378** or by email: [RPAresponse@CyberClan.com](mailto:RPAresponse@CyberClan.com)
  - You will receive a guaranteed response within 15 minutes
  - Incident information will be recorded, advice will be provided and any critical ongoing incidents will be contained where possible
  - Subject to the claim being determined as valid, an expert Incident Response team will be deployed to rapidly respond to the incident, providing Incident Response services including: forensic investigation services and support in bringing IT operations securely back up and running.
- Inform the National Cyber Security Centre (NCSC) - <https://report.ncsc.gov.uk>
- Contact your local police via Action Fraud [Action Fraud website](#) or call **0300 123 2040**
- If you are a part of a Local Authority (LA), they should be contacted
- Contact your Data Protection Officer
- Consider whether reporting to the [ICO is necessary](#) report at [www.ico.org.uk](http://www.ico.org.uk) **0303 123 1112**
- Contact the Sector Security Enquiries Team at the Department for Education by emailing: [sector.securityenquiries@education.gov.uk](mailto:sector.securityenquiries@education.gov.uk)

**Please be aware that speed is of critical importance during a cyber incident to help protect and recover any systems that may have been affected and help prevent further spread.**

## Cyber Recovery Plan

5. Verify the initial incident report as genuine and record on the [Incident Recovery Event Recording Form](#) at Appendix C.
  6. Assess and document the scope of the incident using the [Incident Impact Assessment](#) at Appendix A to identify which key functions are operational / which are affected.
  7. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
  8. In order to assist data recovery, if damage to a computer or back up material is suspected, staff **should not**:
    - Turn off electrical power to any computer.
    - Try to run any hard drive, back up disc or tape to try to retrieve data.
    - Tamper with or move damaged computers, discs or tapes.
  9. Contact [RPA Emergency Assistance Helpline](#).
  10. Start the [Actions Log](#) to record recovery steps and monitor progress.
  11. Convene the [Cyber Recovery Team](#) (CRT).
  12. Liaise with IT staff to estimate the recovery time and likely impact.
  13. Make a decision as to the safety of the school remaining open.
    - *This will be in liaison with relevant Local Authority Support Services / Trust*
  14. Identify legal obligations and any required statutory reporting e.g., criminal acts / reports to the Information Commissioner's Office in the event of a data breach.
    - *This may involve the school's Data Protection Officer and the police*
  15. Execute the [communication](#) strategy which should include a media / press release if applicable.
    - *Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.*
  16. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.
  17. Upon completion of the process, evaluate the effectiveness of the response using the [Post Incident Evaluation](#) at Appendix D and review the Cyber Recovery Plan accordingly.
  18. Educate employees on avoiding similar incidents / implement lessons learned.
- Ensure this plan is kept up-to-date with new suppliers, new contact details, and changes to policy.**

The following sections should be completed to produce a bespoke Cyber Recovery Plan for your school:

## Cyber Recovery Team

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

	Name	Role in School	Contact Details
Recovery Team Leader			
Data Management			
IT Restore / Recover			
Site Security			
Public Relations			
Communications			
Resources / Supplies			
Facilities Management			

*This procedure should not be published with contact details included due to the risk of a data breach.*

## Server Access

Please detail all the people with administrative access to the server.

Role	Name	Contact Details
Headteacher		
School Business Manager		
IT Support Technician		
Third Party IT Provider		

*This procedure should not be published with contact details included due to the risk of a data breach.*

## Management Information System (MIS) Admin Access

Please detail all the people with administrative access to the MIS

MIS Admin Access	Name	Contact Details
Headteacher		
School Business Manager		
MIS Provider		
Data Manager		

*This procedure should not be published with contact details included due to the risk of a data breach.*

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

## Backup Strategy

School Process	Backup Type (include on-site / off-site)	Frequency
Main File Server		
School MIS	Cloud managed service should be able to access anywhere from an Internet Connection. [Bromcom have dedicated back-up server to back up system state & off-line retention of old backups.]	Full – weekly & incremental daily.
Cloud Services		
Third Party Applications / Software installed on the onsite server B2B		
Email Server		
Curriculum Files		
Teaching Staff Devices		
Administration Files		
Finance / Purchasing	Cloud Managed Service which is accessible anywhere from an Internet Connection. [Access Education & Budgeting run 4 different backups across 2 different data centres]	Daily at 15 minute intervals, weekly & monthly
HR / Personnel Records	See MIS	
Inventory		
Facilities Management / Bookings		
Website		
USBs / portable drives		

## Key Contacts

Supplier	Contact / Tel Number	Account / Reference Number
Internet Connection		
Backup Provider		
Telecom Provider		
Website Host		
Electricity Supplier		
Burglar Alarm		
Text Messaging System		

Action Fraud		
Local Constabulary		
Legal Representative		
LA / Trust Press Officer		

*This procedure should not be published with contact details included due to the risk of a data breach.*

## Staff Media Contact

Assigned staff will co-ordinate with the media, working to guidelines that have been previously approved for dealing with post-disaster communications.

The staff media contact should only provide verified facts. It is likely that verifying details will take some time and stating, "I don't know at this stage", is a perfectly acceptable response.

It is likely the following basic questions will form the basis of information requests:

- What happened?
- How did it happen?
- What are you going to do about it?

Staff who have not been delegated responsibility for media communications **should not respond** to requests for information and should refer callers or media representatives to assigned staff.

Assigned Media Liaison(s):

Name: \_\_\_\_\_ Role: \_\_\_\_\_

Name: \_\_\_\_\_ Role: \_\_\_\_\_



## Key Roles and Responsibilities

Every school is unique and the structure and staffing levels will determine who will be assigned which task. This example will help you assign roles and responsibilities, but this is not an exhaustive or a definitive list.

### Headteacher / Principal (with support from Deputy Head / Vice Principal)

- Seeks clarification from person notifying incident.
- Sets up and maintains an incident log, including dates / times and actions.
- Convenes the Cyber Recovery Team (CRT) to inform of incident and enact the plan.
- Liaises with the Chair of Governors.
- Liaises with the school Data Protection Officer.
- Convenes and informs staff, advising them to follow the 'script' when discussing the incident.
- Prepares relevant statements / letters for the media, parents / pupils.
- Liaises with School Business Officer / Manager to contact parents, if required, as necessary

### Designated Safeguarding Lead (DSL)

- Seeks clarification as to whether there is a safeguarding aspect to the incident.
- Considers whether a referral to Cyber Protect Officers / Early Help / Social Services is required.

### Site Manager / Caretaker

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

### School Business Officer / Manager

- Ensures phone lines are operative and makes mobiles available, if necessary – effectively communicating numbers to relevant staff.
- Ensures office staff understand the [standard response](#) and knows who the media contact within school is.
- Contacts relevant external agencies – RPA Emergency Assistance / IT services / technical support staff
- Manages the communications, website / texts to parents / school emails.
- Assesses whether payroll or HR functions are affected and considers if additional support is required.

### Data Protection Officer (DPO)

- Supports the school, using the school data map and information asset register to consider whether data has been put at risk, is beyond reach, or lost.
- Liaises with the Headteacher / Chair of Governors and determines if a report to the ICO is

necessary.

- Advises on the appropriateness of any plans for temporary access / systems.

## Chair of Governors

- Supports the Headteacher throughout the process and ensure decisions are based on sound judgement and relevant advice.
- Understands there may be a need to make additional funds available – have a process to approve this.
- Ensures all governors are aware of the situation and are advised not to comment to third parties / the media.
- Reviews the response after the incident to consider changes to working practices or school policy.

## IT Lead / IT Staff

**Depending upon whether the school has internal or outsourced IT provision, the roles for IT Co-ordinators and technical support staff will differ.**

- Verifies the most recent and successful backup.
- Liaises with the RPA Incident Response Service to assess whether the backup can be restored or if server(s) themselves are damaged, restores the backup and advises of the backup date and time to inform stakeholders as to potential data loss.
- Liaises with the Headteacher as to the likely cost of repair / restore / required hardware purchase.
- Provides an estimate of any downtime and advises which systems are affected / unaffected.
- If necessary, arranges for access to the off-site backup.
- Protects any records which have not been affected.
- Ensures on-going access to unaffected records.

## Teaching Staff and Teaching Assistants

- Reassures pupils, staying within agreed [pupil standard response](#)
- Records any relevant information which pupils may provide.
- Ensures any temporary procedures for data storage / IT access are followed

## Critical Activities - Data Assets

List all the data assets your school has access to and decide which are critical and how long you would be able to function without each one. This could be a matter of a few hours or a matter of a day, a week or even a month.

Complete the required column with the timescale you believe is necessary for recovery. You may find it helpful to refer to your Inventory / Data Map.

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

Also decide if there are any temporary workarounds or if outsourcing is possible. It is useful to consider the cost of any additional resources which may be required in an emergency situation.

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Leadership and Management	Access to Headteacher's email address		
	Minutes of SLT meetings and agendas		
	Head's reports to governors (past and present)		
	Key stage, departmental and class information		
Safeguarding / Welfare	Access to systems which report and record safeguarding concerns		
	Attendance registers		
	Class groups / teaching groups, and staff timetables		
	Referral information / outside agency / TAFs		
	Child protection records		
	Looked After Children (LAC) records / PEPs		
	Pupil Premium pupils and funding allocations		
Medical	Pastoral records and welfare information		
	Access to medical conditions information		
	Administration of Medicines Record		
Teaching	First Aid / Accident Logs		
	Schemes of work, lesson plans and objectives		
	Seating plans		
	Teaching resources, such as worksheets		
	Learning platform / online homework platform		
	Curriculum learning apps and online resources		
	CPD / staff training records		
SEND Data	Pupil reports and parental communications		
	SEND List and records of provision		
	Accessibility tools		
	Access arrangements and adjustments		
Conduct and Behaviour	IEPs / EHCPs / GRIPS		
	Reward system records, including house points or conduct points		
	Behaviour system records, including negative behaviour points		
	Sanctions		
	Exclusion records, past and current		
	Behavioural observations / staff notes and incident records		

Critical Activities	Data item required for service continuity	When Required	Workaround? (Yes / No)
Assessment and Exams	Exam entries and controlled assessments		
	Targets, assessment and tracking data		
	Baseline and prior attainment records		
	Exam timetables and cover provision		
	Exam results		
Governance	School development plans		
	Policies and procedures		
	Governors meeting dates / calendar		
	Governor attendance and training records		
	Governors minutes and agendas		
Administration	Admissions information		
	School to school transfers		
	Transition information		
	Contact details of pupils and parents		
	Access to absence reporting systems		
	School diary of appointments / meetings		
	Pupil timetables		
	Letters to parents / newsletters		
	Extra-curricular activity timetable and contacts for providers		
	Census records and statutory return data		
Human Resources	Payroll systems		
	Staff attendance, absences, and reporting facilities		
	Disciplinary / grievance records		
	Staff timetables and any cover arrangements		
	Contact details of staff		
Office Management	Photocopying / printing provision		
	Telecoms - school phones and access to answerphone messages		
	Email - access to school email systems		
	School website and any website chat functions / contact forms		
	Social media accounts (Facebook / Twitter)		
	Management Information System (MIS)		
	School text messaging system		
	School payments system (for parents)		
	Financial Management System - access for orders / purchases		
Site Management	Visitor sign in / sign out		
	CCTV access		
	Site maps		
	Maintenance logs, including legionella and fire records		
	Risk assessments and risk management systems		
	COSHH register and asbestos register		
Catering	Contact information for catering staff		
	Supplier contact details		
	Payment records for food & drink		
	Special dietary requirements / allergies		
	Stock taking and orders		

## 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:

<b>Operational</b>	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 <b>or</b> teaching and learning) to <b>some</b> 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.
<b>Informational</b>	No Breach	No information has been accessed / compromised or lost.
	Data Breach	Access or loss of data which is <b>not</b> 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)
<b>Restoration</b>	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 a victim of [a cyber-attack / serious system outage]. This has taken down [some / all] of the school IT systems. This means that we currently do not have any access to [telephones / emails / server / MIS etc] At present we have no indication of how long it will take to restore our systems. [OR it is anticipated it may take XXXX to restore these systems]

We are in liaison with our school Data Protection Officer and, if required, this data breach will be reported to the Information Commissioners Office (ICO) in line with requirements of the Data Protection Act 2018 / GDPR. Every action has been taken to minimise disruption and data loss.

The school will be working with the [Trust / Local Authority], IT providers and other relevant third parties [Department for Education / NCSC / local police constabulary] to restore functionality and normal working as soon as possible.

In consultation with the [Trust / 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,

## School Closure

Dear Parent/Carer,

I am writing to inform you that it appears the school has been a victim of [a cyber-attack / serious system outage]. This has taken down the school IT system. This means that we currently do not have any access to [telephones / emails / server / MIS etc]. At present we have no indication of how long it will take to restore our systems.

We are in liaison with our school Data Protection Officer and this data breach has been reported to the Information Commissioners Office (ICO) in line with the requirements of the Data Protection Act 2018 / GDPR.

In consultation with the [Trust / Local Authority] we have completed a risk assessment on all areas affected to address concerns surrounding the safeguarding of our pupils and staff.

I feel that we have no option other than to close the school to students on [XXXXXXXXXX]. We are currently planning that the school will be open as normal on [XXXXXXXXXX]

I appreciate that this will cause some problems for parents/carers with regards to childcare arrangements and apologise for any inconvenience but feel that we have no option other than to take this course of action.

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

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

Yours sincerely,



## Staff Statement Open

The school detected a cyber-attack on [date] which has affected the following school IT systems:

(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will remain open with the following changes to working practice:

(Detail any workarounds / changes)

The school is in contact with our Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, limit severity, and restore systems.

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

## Staff Statement Closed

The school detected a cyber-attack on [date] which has affected the following school IT systems:

(Provide a description of the services affected)

Following liaison with the [Trust / LA] the school will close to pupils [on DATE or with immediate effect].

(Detail staff expectations and any workarounds / changes or remote learning provision)

The school is in contact with our Data Protection Officer, and we have reported the incident to the ICO, in line with the statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities. If you are asked for any information as part of the on-going investigation, please provide it promptly. The school has taken immediate action to mitigate data loss, however we are unsure when systems will be restored. Staff will be kept informed via [telephone / email / staff noticeboard].

All staff are reminded that 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].

## Media Statement

[Inset school name] detected a cyber-attack on [date] which has affected the school IT systems. Following liaison with the [Trust / LA] the school [will remain open / is currently closed] to pupils.

The school is in contact with their Data Protection Officer and will report to the ICO, if necessary, in line with statutory requirements of the Data Protection Act 2018 / GDPR.

This incident is being investigated by the relevant authorities and the school has taken immediate remedial action to limit data loss and restore systems.

A standard staff response for serious IT incidents should reflect only information which is already freely available and has been provided by the school in initial media responses.

### Standard Response

The information provided should be factual and include the time and date of the incident.

Staff should not speculate how long systems will take to be restored but can provide an estimate if this has been agreed.

If no restoration date has been advised, staff should merely state that work is on-going and that services will resume as soon as practically possible.

Staff should direct further enquiries to an assigned contact / school website / other pre-determined communication route.

### Standard Response for Pupils

For staff responding to pupil requests for information, responses should reassure concerned pupils that incidents are well prepared for, alternative arrangements are in place and that systems will be back online shortly.

Staff should address any outlandish or suggested versions of events by reiterating the facts and advising pupils that this has been confirmed in letters / emails to parents / carers.

Staff should not speculate or provide pupils with any timescales for recovery, unless the sharing of timescales has been authorised by senior staff.

## Appendix C: Incident Recovery Event Recording Form

This form can be used to record all key events completed whilst following the stages of the Cyber Response Plan.

<b>Description or reference of incident:</b>	
<b>Date of the incident:</b>	
<b>Date of the incident report:</b>	
<b>Date/time incident recovery commenced:</b>	
<b>Date recovery work was completed:</b>	
<b>Was full recovery achieved?</b>	

### Relevant Referrals

Referral To	Contact Details	Contacted On (Time / Date)	Contacted By	Response

### Actions Log

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

## Appendix D: Post Incident 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:		