




Cyber Security Policy

Policy Originator	LGfL
Governor Responsible	Premises and Resource Committee
Status	Statutory
Last reviewed	Spring 2024
Ratified on	16.05.2024
Review period	Annually
Signed by Governor	

Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity Policy outlines Campsbourne School's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Scope of Policy

This policy applies to all Campsbourne School's staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk Management

Campsbourne School will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to the Resources and Premises Committee 3 times a year.

Physical Security

Campsbourne School will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Campsbourne School will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform Turn It On and the Head Teacher as soon as possible. Personal accounts should not be used for work purposes. Campsbourne School will implement multi-factor authentication where it is practicable to do so.

Devices

To ensure the security of all Campsbourne School issued devices and data, users are required to:

- Lock devices that are left unattended

- Update devices when prompted
- Report lost or stolen equipment as soon as possible to the School Office.
- Change all account passwords at once when a device is lost or stolen (and report immediately to Turn It On and the Head Teacher)
- Report a suspected threat or security weakness in Campsbourne School's systems to Turn It On and the Head Teacher.

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software [e.g. Sophos and Malwarebytes for LGfL schools – see sophos.lgfl.net / malwarebytes.lgfl.net]
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

Data Security

Campsbourne School will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Campsbourne School defines confidential data as:

- [Personally identifiable information](#) as defined by the ICO
- [Special Category personal data](#) as defined by the ICO
- Unpublished financial information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology

- 3 versions of data
- 2 different types of media (Disk and Cloud Storage)
- 1 copy offsite/offline

[LGfL provide Gridstore as an online backup – see gridstore.lgfl.net]

Sharing Files

Campsbourne School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Wherever possible, keeping Campsbourne School's files on school systems
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels

- Alerting [IT Support/DPO] to any breaches, malicious activity or suspected scams

Training

Campsbourne School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a “No Blame” culture towards individuals who may fall victim to sophisticated scams. [LGfL offer [Cyber Security Training for School Staff](#) and [Sophos Phish](#), a phishing simulation tool that links to training material]

System Security

Turn It On will build security principles into the design of IT services for Campsbourne School.

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors’ & staff personal devices from school systems
- Review the security risk of new systems or projects

Major Incident Response Plan

Campsbourne School will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. This will include identifying or carrying out:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)

Maintaining Security

Campsbourne School understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Campsbourne School will budget appropriately to keep cyber related risk to a minimum.

Appendix A

Appendix A highlights the top ten cybersecurity risks to Campsbourne School. It details the actions that are being taken to reduce their impact & likelihood, and any progress that has been made since the beginning of the year.

Section 3 lists the risks that are being actively monitored, and then details the actions that are being taken and progress to reduce the probability and impact of these risks.

The chart in Section 4 shows where the current cybersecurity risks are on a risk heat map.

Recent Incidents

None

Summary of the top risks being monitored 2023/2024

Risk #	Risk description	Probability	Impact	Value
1	Ransomware attack	Low	Very High	20
2	Someone is caught by phishing email	Medium	High	19
3	Password is compromised	Medium	High	19
4	No encryption	High		24
5	Laptop stolen leads to data breach	Medium	Medium	15
6	iPad stolen leads to data breach	Medium	Medium	15
7	Website is hacked	Low	High	16
8	School systems available from the internet are insecure	Medium	High	19

Detailed information of the top risks being monitored

Risk Area 1		Ransomware attack			
Likelihood of occurrence (score)	Low	Severity of impact (score)	Very High	Current Risk Score	20
Action to Mitigate Risk	<ul style="list-style-type: none"> • Implement and test Incident Response plans • Ensure backups are running and tested • Manage & monitor antivirus • Implement Multi Factor Authentication • Maintain the patch management of operating systems and applications • Provide regular cybersecurity training to all staff • Reduce vulnerabilities in our online 'digital footprint' with LGfL's Security School Report 				
After mitigation					
Residual likelihood (score)	Very Low	Severity of impact (score)	High	Risk Score	8
Monitoring process	<ul style="list-style-type: none"> • Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> • January - Implement Multi Factor Authentication • Sept Inset – Provide cybersecurity training 				

Risk Area 2		Someone is caught by phishing email.			
Likelihood of occurrence (score)	Medium	Severity of impact (score)	High	Overall or Gross Risk	19
Action to Mitigate Risk	<ul style="list-style-type: none"> • Training provided by Internet provider to promote awareness and practical steps to avoid further risk. 				
Residual likelihood (score)		Residual Severity of impact (score)		Residual Risk	
Monitoring process	<ul style="list-style-type: none"> • Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> • Further Phish Threat campaigns run periodically to identify risk areas. 				

Risk Area 3		Password is compromised			
Likelihood of occurrence (score)	Medium	Severity of impact (score)	High	Overall or Gross Risk	19
Action to Mitigate Risk	<ul style="list-style-type: none"> • Password reset, devices scanned for virus activity. 				
Residual likelihood (score)		Residual Severity of impact (score)		Residual Risk	
Monitoring process	<ul style="list-style-type: none"> • Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> • Use of more complex passwords or phrases should be used. 				

Risk Area 4		No encryption			
Likelihood of occurrence (score)	High	Severity of impact (score)	Very High	Overall or Gross Risk	24
Action to Mitigate Risk	<ul style="list-style-type: none"> Product such as Egress can be set up for secure data transfer. School is entitled to 15x free licences as part of their LGfL subscription. 				
Residual likelihood (score)		Residual Severity of impact (score)		Residual Risk	
Monitoring process	<ul style="list-style-type: none"> Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> Identify need for encryption tools for data sharing. 				

Risk Area 5		Laptop stolen leads to data breach			
Likelihood of occurrence (score)	Medium	Severity of impact (score)	Medium	Overall or Gross Risk	15
Action to Mitigate Risk	<ul style="list-style-type: none"> Remove device from school network. Block IP address. 				
Residual likelihood (score)		Residual Severity of impact (score)		Residual Risk	
Monitoring process	<ul style="list-style-type: none"> Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> Explore use of tools for monitoring devices 				

Risk Area 6		Tablet stolen leads to data breach			
Likelihood of occurrence (score)	Medium	Severity of impact (score)	Medium	Overall or Gross Risk	15
Action to Mitigate Risk	<ul style="list-style-type: none"> Remove device from school network. Block IP address. 				
Residual likelihood (score)		Residual Severity of impact (score)		Residual Risk	
Monitoring process	<ul style="list-style-type: none"> Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> Explore use of tools for monitoring devices 				

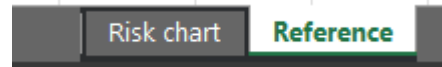
Risk Area 7		Website is hacked			
Likelihood of occurrence (score)	Low	Severity of impact (score)	High	Overall or Gross Risk	16
Action to Mitigate Risk	<ul style="list-style-type: none"> Website company to advise. 				
Residual likelihood (score)		Residual Severity of impact (score)		Residual Risk	
Monitoring process	<ul style="list-style-type: none"> Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> 				

Risk Area 8	School systems available from the internet are insecure				
Likelihood of occurrence (score)	Medium	Severity of impact (score)	High	Overall or Gross Risk	19
Action to Mitigate Risk	<ul style="list-style-type: none"> Security in place Sophos Antivirus and LGfL firewall. 				
Residual likelihood (score)		Residual Severity of impact (score)		Residual Risk	
Monitoring process	<ul style="list-style-type: none"> Will be monitored through half termly meetings with the IT technician and reported to governors at Resources and Premises Committee meetings 				
Further Action/Date	<ul style="list-style-type: none"> Ensure Sophos updated on all devices. LGfL firewall monitored. 				

Cybersecurity Heat Chart

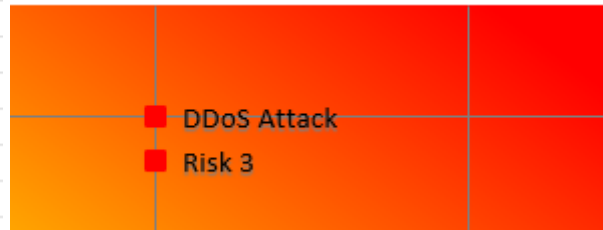
The chart on the next page has been copied from the 'Cybersecurity Risk Assessment Chart' spreadsheet available at <https://elevate.lgfl.net>

Once opened, update the information in the table on the Reference sheet.

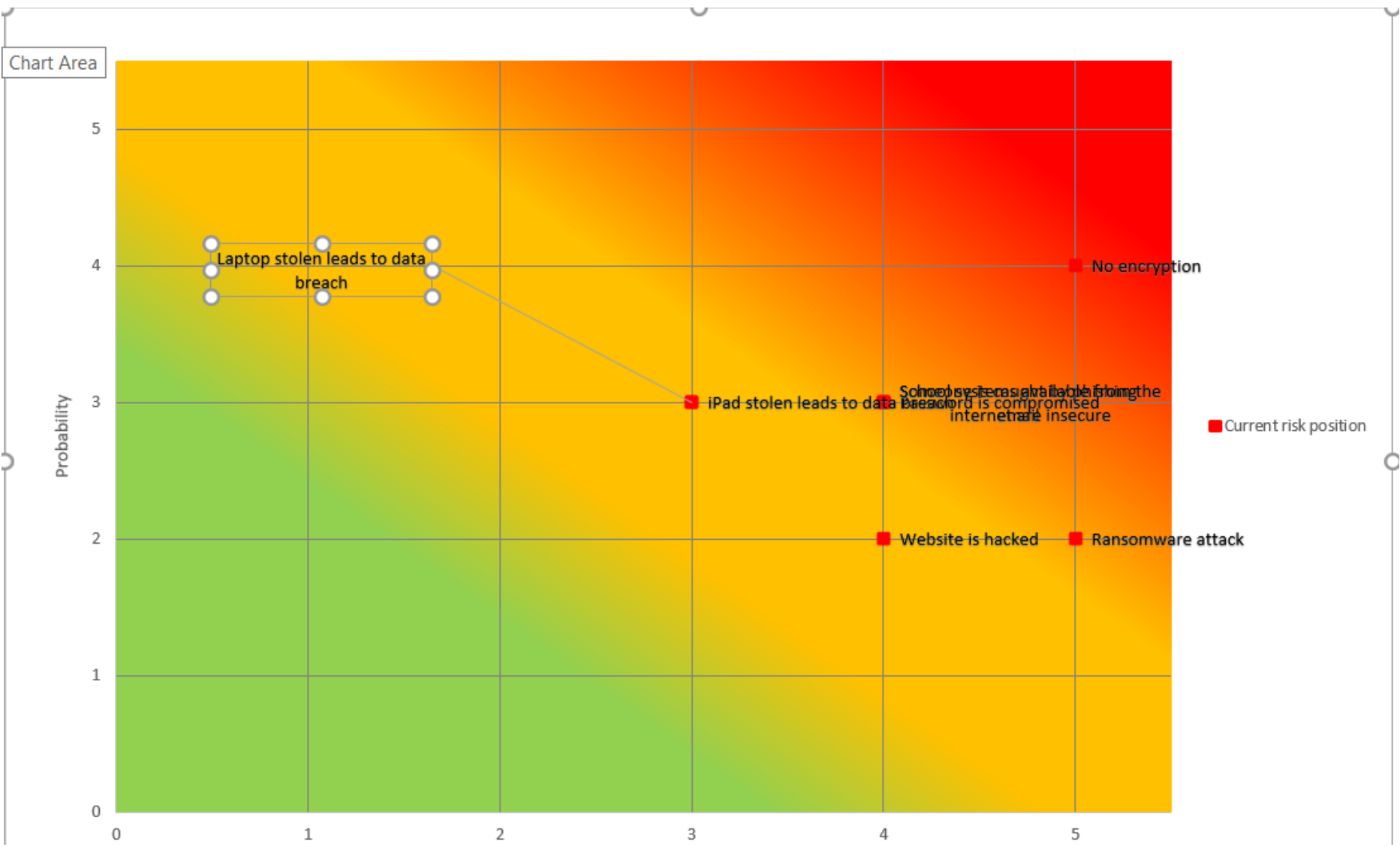


Once the table has been update the chart will reflect your changes. You can even give each risk a friendly name that will then show on the Chart.

	A	B	C
Current risk position		Probability	Impact
Ransomware		3	2
DDoS Attack		5	3
Risk 3		4.8	3
Risk 4		3	3
Risk 5		1	1
Risk 6		4	3
Risk 7		2	5
Risk 8		4	4
Risk 9		1	4
Risk 10		2	3



Once you have updated the table go to the Risk Chart sheet and copy the chart into the document.



Appendix – Common Cybersecurity Terms

Phishing

Phishing is a type of social engineering attack where cybercriminals use email, text messages, or other forms of communication to trick individuals into sharing sensitive information, such as usernames and passwords.

Spoofing

Email spoofing involves forging the "from" address of an email to make it appear as if it were sent from a legitimate contact. This is commonly used during phishing attacks to trick the recipient into trusting fraudulent emails.

Malware

Malware is a type of software that is designed to harm or disrupt computer systems. This can include viruses, worms, Trojan horses, and other malicious programs.

Ransomware

Ransomware is a type of malware that encrypts computer files making them inaccessible. Cybercriminals can then demand payments in exchange for the decryption key.

DDoS

A Distributed Denial of Service attack is when millions of requests are made against a network or website flooding it with traffic, making it unavailable.

Supply chain attack

A supply chain attack is a type of attack that targets a company's suppliers, with the aim of causing disruption or gaining access to sensitive information or systems that may be held by the company.

Firewall


A firewall is a network security device that monitors and controls incoming and outgoing network traffic.

Antivirus

Antivirus software is designed to detect, prevent, and remove malware from a computer.

Security Update/Patch

A security update or patch is an update that fixes security vulnerabilities or other issues.

 Campbourne School	Headteacher	Jonathan Smith
	Chair of Governors	Laura Bunting-Lewis
	Network manager / other technical support	Nick Irving
	Date this policy was reviewed and by whom	[]
	Date of next review and by whom	[]