Haddenham St Mary's Church of England School

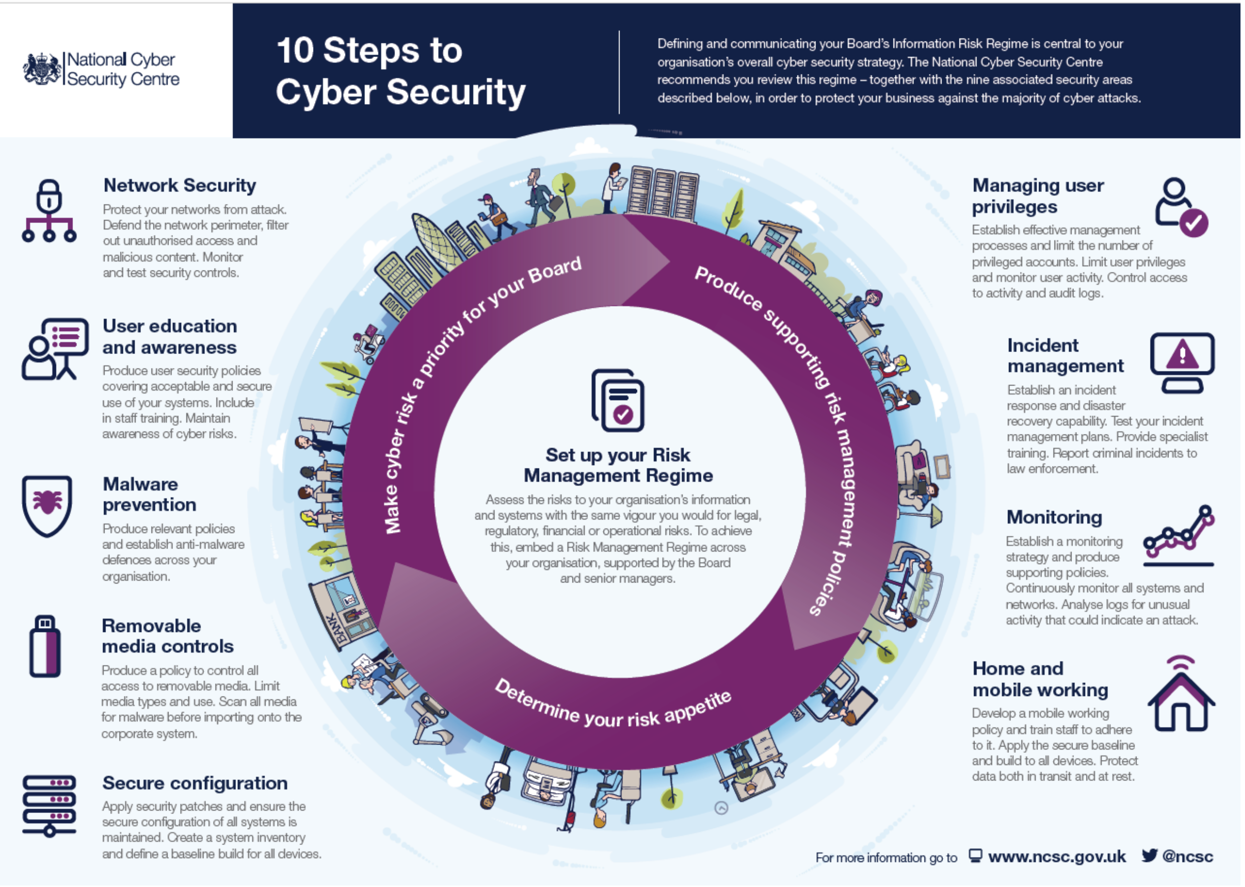
Committed to excellence, care and fun for all.

"Your word is a lamp to guide my feet and a light for my path." (Psalm 119.105)

Haddenham St Mary's CE School, Aston Road,
Haddenham, Aylesbury, Bucks, HP17 8AF. T: 01844 291 455
Headteacher: Mrs. K Collett. Chair of Governors: Mrs. G Bull
office@haddenham-st-marys.bucks.sch.uk

10 steps to cyber security – Haddenham St Mary's CE School evidence, Nov 2020

- This has been completed having sought advice from our ICT support Team at Buckinghamshire Council (SchoolsTST). They are in agreement that in no area of the risk assessment are we at risk. As a school we have taken all precautions necessary and continue to keep up to date with developments via the SchoolsTST team.
- RM provide our internet service and their systems minimise our risks also.



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite
BANK

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

Area	Evidence	Risk assessment
Network Security		
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.	• RM provide our internet and centrally defend our network. • As a school we use RM safety filter to filter out malicious content. • As a school, we can control the websites that are viewed. This is done via an email to RM support. • Each I pad has age appropriate filters applied so that children cannot access inappropriate content. • SchoolsTST monitor our systems and back up our server daily (overnight) using a system called REBUSS.	🟩
User education and awareness		
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.	• We have a staff acceptable user policy and a staff code of conduct which includes use of social media. All staff sign and agree to this. • We have a remote learning whole school agreement in place between parents and staff. Virtual meeting protocols in place for all stakeholders. • Children sign an acceptable user policy and are reminded about internet safety rules as part of the curriculum. • Staff reminded regularly of policies and fully induced when they begin as a member of staff. GDPR training includes a section on cyber security. • GDPR lead reminds staff of cyber risks and emails relevant information to staff.	🟩
Malware prevention		
Produce relevant policies and establish anti-malware defences across your organisation.	• Sophos Endpoint, Sophos Central intercept X are packages offering malware and ransomware protection. These are installed on laptops and desktops in school on the network. SchoolsTST monitors the licences for these. Sophos Central Intercept X is installed on machines deemed most at risk. • Staff advised not to open any emails that they are unsure about. Staff only use work emails and accounts for school based activities. Emails monitored and filtered by RM. • Staff are requested not to bring unknown USB devices into school.	🟩

Removable media controls		
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the school system.	• Staff who may need an encrypted memory stick are issued with one when they start their role. This is password protected. • All staff are requested not to bring in unknown removable media/USB pens into school. • A USB pen is issued per classroom for use on the Clevertouch board to access resources from the T drive. • Each laptop/desktop machine in school is encrypted using a Bit locker program. • All sensitive data is only kept on the school central server and staff do not keep such data on their laptops. • Removable devices are scanned before using.	🟩
Secure configuration		
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.	• All devices are built and purchased through SchoolsTST. • SchoolsTST have a standard build specification for any new devices. • All devices are patched on a monthly basis as per the Microsoft/Datto schedule that SchoolTST work to. This is an automatic process that runs within the Windows operating system. • A system inventory is maintained by SchoolsTST with P numbers for machines (this is their system for remote log on identification).	🟩
Managing user privileges		
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.	• Our system is managed by SchoolsTST and they set up and delete staff users and privileges on school's request. • Each staff member has their own log on profile with access to specific parts of the server as needed. • Only SLT/office staff have access to confidential files via user privilege. • No one in school can set up network access so this means that the system stays secure. • RM has placed software on our server linked to RM Unify to allow SIMS to access user privileges for children. • Senior staff in school can manage children's and teachers Office 365 accounts and privileges re use of Teams.	🟩

Incident management		
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.	• We have an Emergency Planning policy including Business continuity plan – last reviewed Jan 2019. • All our systems and servers are backed up on a daily basis by REBUSS through SchoolsTST so there would be minimal loss of critical information that would only span 1 day potentially. • Governance and important documents are saved electronically on GovernorHub. • If we had any criminal incidents we would work with the police.	🟩
Monitoring		
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.	• RM monitor our systems and networks and analyse for any unusual activity. • Unknown people don't enter the schools site and use the school machines. • SchoolsTST monitor and update our antivirus software on a regularly basis.	🟩
Home and mobile working		
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.	• Home working policy embedded within Data Protection policy. • Staff asked to log on to laptops and devices in school and properly shut down and log on before taking laptops home. • Only teachers and admin staff have a laptop designated to them for use at home. • Each laptop is secured with a user profile. • Teachers only use encrypted memory sticks to move sensitive data and only when needed. • Admin and SLT have access to Datto system that allows remote log on to central server from home.	🟩