Cyber Aware Security Audit

	Compliance Status
School Name: OLASP	Fully
Audit Date: 18/3/22	Partial
	None
	N/A

Section 1: Patching Systems

Action	Compliance	Notes	Action
Are all staff devices installed with operating systems of current or one previous generation? (windows 11 or 10)	Fully		
Are Windows updates install on all staff devices automatically or on a minimum monthly basis?	Fully		
Are servers installed with operating systems supported by Microsoft? (Windows Server 2022, 2019 or 2016?)	Fully		
Are Windows updates install on servers automatically or on a minimum monthly basis?	Fully		
Is up to date Anti Virus software installed on all Windows devices	Fully		
Is up to date Anti Virus software installed on all Windows Servers	Fully		

Section 2: Improving access controls and enabling multi-factor authentication

Action	Compliance	Notes	Action
Are lock screen controls implemented on staff laptops?	Fully		
Are all staff devices installed with Bitlocker (or similar) encryption security?	Fully		
Are strong passswords enforced for staff Windows User accounts	Fully		
Are strong passswords enforced for staff O365/Google Email Accounts	Fully		
Is Two Factor Authetication enforced for staff O365/Google Email accounts	Partial		Need to force this to on for O365 Tenant before 03/02/2023

Have all O365/Google accounts been checked to remove/disable any dormant accounts?	Fully		
Is there Risk Based Security settings in place for O365/Google systems for brute force attacks?	Fully		
Are other cloud platform accounts setup with Two Factor Authentication (eg CPOMS, Arbor etc)	Fully		
Is there a remote access solution in place and does this have Two Factor Authentication?	Fully		
Is Geoblocking enforced for all Non UK countries in the firewall/filter system?	Fully		

Section 3: Checking that backups and restore mechanisms are working

Action	Compliance	Notes	Action
Is there an offline backup of all server data in place with regular drive rotation?	Fully		
How often are offline drives rotated? (minimum weekly)	Fully - Weekly		
Is there an offsite cloud copy of server data in place with at least weekly update?	Fully		
Are backup successful/unsuccessful reports setup to notify a key contact at school?	Fully		
Is there a process to check back status and recitfy issues?	Fully		

Section 4: Implementing an effective incident response plan

Action	Compliance	Notes	Action
Do you have access to your key system passwords in the event of a disaster?	Fully		
Is there a disaster recovery plan in place?	Partial		Need to finish Disaster Recovery Plan by 03/02/2023
Is there a process to test the disaster recovery plan?	Partial	In the process of writing this up	Need to finalise plan to test recovery plan by 03/02/2023

Section 5: Ensuring that online defences are working as expected			
Action	**Compliance**	**Notes**	**Action**
Has the NCSC password monitor been run to check staff passwords for common password strings?	Partial		Need to re-run for 2023 by 03/02/2023
Has the Microsoft attack simulator been used to check security defences are working as	Partial		Need to re-run for 2023 by 03/02/2023
Section 6: Keeping up to date with the latest threat and mitigation information			
Action	**Compliance**	**Notes**	**Action**
Has basic cyber awareness staff training been completed?	Partial	Forward Training Video for staff	Forward Training Video for staff by 03/02/2023