Appendix C (update)

Cyber Security 2018/19 **Final report issued January 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
01	Management should put a defined plan in place to address all existing critical and high priority vulnerabilities in a timely manner. There should be a defined procedure in place to resolve vulnerabilities as and when they are encountered.	Medium	Update existing procedures to review and remediate vulnerabilities (other than MS patches). If required, implement additional system e.g. SCCM to manage deployment of "other" vulnerabilities. Position (March 2019) Review of products such as SCCM to manage 3rd party patching across the estate.	Head of ICT	30 November 2019	×	

Cyber Security 2018/19 **Final report issued January 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			Position (July 2019) In progress. Currently managed on a ¼ basis, using Qualys vulnerability software to assess and scan with manual remediation via patching. System will be put in place to automate where possible.				
02	There should be a mechanism to restrict any non-complying devices to connect to the Council's IT network.	Medium	Review current AV and VPN solution and viability to restrict devices with no up to date protection from connecting to the network fully. Ensure that daily reports for AV protection are monitored against asset register and this is	Head of ICT	30 September 2019	× Part resolved. Extension requested to deploy new	30 December 2019

Cyber Security 2018/19 **Final report issued January 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
	Additionally, there should be continuous monitoring in place for all devices connected on the network to be fully antivirus protected.		reported to the ICT Section Head. Position (March 2019) Reporting mechanism from Infrastructure monitoring through to desktop services is in place. Mechanism to ensure that desktop services remediate the gaps sufficiently is currently underway. Replacement VPN, for all homeworking, is within scope for replacement Wide Area Network. New VPN solution will review ability to ensure that all connected devices have up to date AV.			remote working solution.	

Cyber Security 2018/19 **Final report issued January 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			Position (July 2019) Continuous AV monitoring in place. Daily reports reviewed to ensure all connected devices have the most recent signatures. Where the signature has not been applied this is flagged and remediated by an engineer. New remote working solution has AV checker within Enterprise Management module. Request to extend the new remote working solution roll out to December 2019. The rollout				

Cyber Security 2018/19 **Final report issued January 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
			will have commenced in August 2019, but needs to be deployed to all users across all sites, in line with the deployment of new personal IT kit and Unified Communications.				
03	A training needs assessment should be performed for all members of staff that have responsibility for Cyber security so as to determine their training needs. Compliance should be monitored and action taken when members of staff are found to have not	Medium	Review current skills against role to assess gap, recommending appropriate training as an outcome. Note funding will have to be approved. HR Manager Monitor and report against all staff who have not completed the annual requirement to refresh knowledge via the Security awareness programme.	Head of ICT	30 September 2019 June 2019	× ✓	

Cyber Security 2018/19 **Final report issued January 2019**							
Ref No.	Recommendation	Priority	Action to Date	Responsibility	Deadline	Resolved × or ✓	Revised Deadline
	completed the IT Security and Data Protection training.		Position (March 2019) New Learning Management system will be ready approximately April 2019. This is led by the HR service. Once in place more accurate reporting mechanisms can be used to ensure staff are completing the required mandatory training. **Position (July 2019)** Monitoring regarding mandatory training completed now in place via new Learning Management system. Skills gap assessment ongoing.				